CHAPTER: Operations, Internal Controls, Audit and Information Technology

SECTION: Introduction to Operations and Internal Controls — Section 300

Introduction to Operations and Internal Controls

The operations area of the trust department is the focal point for all actions affecting trust and asset management accounts. All transactions initiated by the various areas of the department usually require some type of action by trust operations. Given the complexity and expense of the different trust operational systems, many trust departments now choose to outsource one or more of their operational functions. If such a choice is made, examiners should look for strong oversight and established internal controls.

The operations area has three major functions: 1) safekeeping and custody; 2) transaction processing and recordkeeping; and 3) regulatory compliance and reporting. The accounting system(s) required to handle these three broad areas of responsibility is extremely complex. It must be able to furnish detailed account information regarding the department's accounts to management, customers and regulatory agencies. The system of internal controls must ensure that records are accurate and assets are properly safeguarded. The system of processing assets, such as moving purchases or sales through the trading area or into or out of the vault, must also ensure that assets are properly safeguarded.

Operations and Internal Controls

"Operations" refers to the trust department's systems and procedures for implementing custody, collection, payment, reporting and processing. "Internal controls" refers to the systems and procedures, checks and balances, communication lines and warning signals, for safeguarding the customer assets under the control of the department through all the various phases of operations activity. Operations and internal controls are therefore closely related and must be evaluated together.

In evaluating the operations function, efficiency should be weighed against the adequacy and effectiveness of controls and safeguards. A highly efficient operation that is devoid of proper controls and safeguards poses a serious threat to the safeguarding of funds and securities and should be evaluated accordingly. Similarly, excessive or cumbersome controls may adversely impact the efficiency of operations, thereby affecting the quality of service to customers. Another consideration is that controls and audits tend to complement one another and weaknesses in one may be compensated for by strengths in the other. Despite the ideal of strict separation of the auditing and operations functions, internal auditors, particularly in smaller departments, may still perform duties such as reconcilements. In other savings associations these duties are performed exclusively by a separate operations or control unit. Thus, examiners should accept any arrangement as long as it is effective.

While operations and internal controls may vary widely from institution to institution based on the size and character of its trust and asset management business and the individual systems used, certain basic principles and controls should be in any system. Specifically, an effective system of operations and internal controls must ensure that:

- assets are adequately safeguarded;
- accounting data is accurate and reliable;
- timely information on accounts is available or can be provided;

- operating efficiency is maintained at an acceptable level;
- new financial products, services and future department growth are accommodated; and
- applicable law is followed.

The types of internal controls that are required depend upon the size and organization of the department. While it is not possible to outline specific control procedures, certain basic control devices should be found in varying degrees. These controls are discussed throughout this section. Examples of basic controls include separation of duties; accounting controls; controls over receipts and disbursements; dual control over assets; and asset and security movement controls.

Savings associations of all sizes must ensure that they maintain a strong control environment that influences the control consciousness of their personnel. This is the foundation of internal control and provides sound discipline and structure. Internal control environment factors include a well-defined organizational structure and workflow; proper audit coverage; defined integrity and ethical values; and sound written policies and procedures.

Larger departments should have a clearly defined organizational structure that provides the framework within which operations activities are planned, executed and monitored. Key areas of authority and responsibility should be established, as well as appropriate lines of reporting.

Books and Records

There are two statutory and regulatory requirements applicable to trust department books and records. First, HOLA requires a savings association to "keep a separate set of books and records" for its trust department (§5(n)(2)). That law is implemented by 12 CFR §550.430, which requires that a savings association "shall keep its fiduciary records separate and distinct from your other records." These requirements, coupled with the corollary requirement to segregate trust department assets from the savings association's own assets underpin one of the basic tenets of a trust and asset management relationship; these assets are not owned by the savings association and are not to be treated as assets of the savings association. Thus, if a savings association becomes insolvent, trust and asset management assets do not form part of the general assets of the savings association and are not subject to the claims of creditors.

The second statutory requirement that relates to trust department books and records is that records must show "in proper detail all transactions" or, as implemented by 12 CFR §550.410, the fiduciary "must keep adequate records for all fiduciary accounts." Adequate books and records are discussed in various contexts throughout the remainder of this chapter.

Separation of Duties

One of the basic principles of sound operations and internal controls is that of separation of duties and responsibilities. Simply put, this means that no one individual should be responsible for, or have complete control over, any transaction from beginning to end. Therefore, one individual should not be capable of authorizing, initiating and/or executing a transaction and then reviewing it for appropriateness. In a trust department, this concept begins by segregating administrative from operational functions and continues by segregating duties within the operating system itself. Adherence to this principal not only reduces the occurrence of unintended errors and mistakes but also reduces the opportunity for theft or embezzlement. For example, if one individual is responsible for all phases of check writing, the possibility exists that

through a combination of double or dummy entries and forgeries, the individual could obtain the proceeds of the check.

The extent that organizational functions and individual personnel duties are separated will depend primarily upon the size of the department. In larger departments, the volume of activity itself dictates the separation of duties. In other words, because of the amount of work, each employee typically performs only one task. In smaller departments, such a separation of duties may not be feasible since one person is usually required to do a number of tasks. Examiner judgment must be used in these instances to evaluate whether or not the department maintains an acceptable system of checks and balances. Size alone is not a valid reason for failing to implement at least minimal and basic internal control features.

Trust Accounting Principles

While accepted accounting principles apply generally to trust department recordkeeping, significant differences exist between the accounting systems used by the trust department and the savings association's other departments. Trust accounting does much more than just keep track of debits and credits. Trust accounting for example, must further distinguish debits and credits into income and principal. In addition, trust accounting involves keeping records of asset transactions, including the basis and market value of securities held by personal trust accounts. Another major difference is that the accounting for certain transactions may be mandated by either the governing document or by state law.

The most important detail regarding trust accounting is that each of the trust department's accounts must be treated as an individual entity. However, the accounting system adopted by the trust department must reflect not only a statement of condition for individual accounts but also aggregate statements for the department as a whole. Therefore, because the trust department does not account for its own assets but rather for the property of others, the "normal" accounting principal of assets minus liabilities equals capital, does not apply. Instead, a shorthand equivalent expression would be assets equal accountability (or liabilities). For trust accounting purposes, a trust department's assets consist of all the property being held in individual accounts. Similarly, its liabilities consist of the carrying value of all the individual accounts. Stated another way, a department's assets, its securities, deposits, real property, etc. held by it for others, are also its liabilities, since the department is accountable (liable) to others for those assets.

Accounting control is achieved by balancing individual account ledgers against the trust department's general ledger. Certain activity relating to the trust department should also be included in the savings association's general ledger and financial statements. For example, cash balances in individual accounts, which are deposited with the savings association in demand and time deposit accounts, revenues and expenses of the trust department may be recorded on its general ledger.

Accounting Systems and Records

In order to effectively administer its trust accounts, trust operations in general must provide comprehensive and detailed recordkeeping and information systems. Accounting systems within a trust department may range from hand-posted records to sophisticated electronic data processing systems. Such systems may be developed within a trust operations department or utilized on an outsourced basis. According to the AICPA's Industry Audit Guide, the accounting records of a trust department should, at least, reflect the asset holdings and liabilities of each customer, the status of each trust account and all transactions relating to each account. This requires records relating to the trust department's total asset holdings and total liability, which will be in its general ledger. It also requires records that can provide detailed information for each trust

account, including: income; principal; transactions related to investments; and lists of assets held by amount and type. The information for each of these categories will most likely be in a separate control account. The values at which assets of the various trust accounts are carried on the ledger may vary. These values may include: nominal value ($1 for control purposes); cost or basis (for tax purposes); or market value.

As mentioned above, the sophistication of the trust department as well as the accounting systems utilized will vary in relation to the size and character of accounts administered. However, the recordkeeping concepts and principles involved remain the same: trust records must be maintained so as to clearly reflect the interests of the various accounts and to permit a thorough and satisfactory examination.

The following information typically appears in trust department records, as applicable, for each asset held by the trust department:

- CUSIP or property number
- Asset description
- Asset type
- Basis (or cost) for tax purposes
- Market price
- Interest rate and maturity date

Trust department records should generally consist of the following:

- ***General ledger***. The general ledger will comprise all control accounts of the department. It includes both customer as well as internal accounts used by the department to facilitate its operation. Many automated systems have subsidiary control records but do not have the traditional "general ledger."
- ***Asset control accounts***. These accounts should reflect total holdings of major asset categories, such as stocks, bonds or deposits.
- ***Subsidiary asset controls***. These accounts will reflect total investments in specific issues of stocks, bonds, etc.
- ***Liability control accounts***. These accounts will reflect the total of cash and investment holdings of each type of account administered. This category should be further subclassified to allow the department to post transactions to individual accounts. The cash ledger should detail income and principal cash and reflect transactions in chronological sequence. The investment ledger should reflect each asset held by a trust account. Purchase, sales, stock dividends and splits should be recorded in chronological order.
- ***Journals, ledgers, files and other records of original entry***. While these records may also be maintained in a variety of forms, they should all furnish the figures which are to be posted to the general ledger or control accounts, provide the basis for the entries which may be made on all other records affected by each transaction and provide a chronological record of all the day's transactions. In a nonautomated system, these records would normally include a blotter and a transaction journal. From these sources, posting is done to individual ledgers, which should in turn be balanced periodically to the general ledger. In an automated system, internal balancing control procedures

should be performed each time the ledgers are posted. These procedures should include the balancing of totals on the transaction journal and verification that ledger records balance to the general ledger.

- ***Individual Account Records***. These records should be maintained for each individual account administered by the department and should reflect transaction histories, list individual assets and provide a total of individual investments and cash for each account.
- ***Other Records***. Other records which affect the operation of a department to a significant degree and which an examiner will find useful in the examination process are a securities transaction register, a vault control log and broker statements. The securities transaction register is a record of all securities transactions listed in chronological order. A vault control log is used to record the dates and identities of individuals who accessed the department's vault. Records should also be maintained indicating which vault contents were accessed and the reasons for the access. Broker statements are similar in some respects to deposit account statements, they reflect all trust department securities transactions. These statements should be reviewed carefully by the department and reconciled to broker confirmations and the bank's securities transaction register.

In addition, there are several other subsidiary accounting records, which should be maintained in all trust departments. They include a digest or synopsis record (which highlights important provisions of the governing instrument such as remittance instructions), a tickler system (which is a chronologically arranged system of records to remind the department of routine and recurring tasks, such as collecting income, distributing funds and calculating fees), security ledgers (which lists securities by issue rather than by individual account), dividend and other claim records (which includes receivables and payables), cash management accounts (which reflect daily cash transactions and balancing) and suspense accounts (which are used to hold transactions for a short time when uncertainty exists as to the correct trust account posting of an income item).

In order to ensure the accuracy and reliability of the department's accounting system, it must be reconciled and controlled on a routine and timely basis. Generally accepted trust department practices normally call for daily posting of account records and ledgers and for, at least, monthly balancing and reconcilements of records and ledgers in a nonautomated department. However, individual circumstances such as the level and type of activity may justify a different timeframe. In most automated systems, ledger controls are internally maintained as part of the system's verification procedures. These procedures normally provide for the automatic, daily balancing of separate asset and liability files. If any discrepancies arise as a result of such balancing, the savings association should begin to promptly research and/or correct.

Principal and Income

A fundamental and significant principle in trust accounting as opposed to other types of accounting is the requirement that separate records must normally be maintained to distinguish between the principal and income of a trust, including principal and income cash. The trust accounting system must ensure that principal and income flow to the intended class of beneficiary. For example, a trust may provide that one or more individuals, referred to as income beneficiaries, are entitled to receive current income of the trust; while other individuals, referred to as remainder beneficiaries or remaindermen, are entitled to the trust property after expiration of the income interest or death of the income beneficiary. However, this distinction is not important for employee benefit trusts as plan participants are entitled to all the benefits of the plan.

The principal (or corpus) of the trust is defined as cash and other property transferred to the trust and any appreciation derived from holding such property. Income is defined as the return derived from the use of

principal, such as (in most cases) dividends, interest, rents or royalties. Income may be distributed as cash or reinvested for the account and held as invested income. The trust agreement often provides specific guidance for allocation of principal and income, usually to the different beneficiaries or to the trust itself. Additional guidance is provided under the applicable state's principal and income act that is based in large part on the Uniform Principal and Income Act. Examiners are reminded that states many times modify "uniform" acts during the legislative process. Consequently, the law of any state may depart in small or large measure from the "uniform" act. To add to the confusion, there are several uniform acts in existence, as it has been amended several times, therefore states have enacted variations of different uniform acts.

Outsourcing Arrangements

Many trust departments find it is financially beneficial to outsource some or all trust accounting functions to third parties or affiliates. Outsourcing of trust operations does not relieve management of its responsibilities to provide oversight and control risks. Outsourcing arrangements present four key challenges, which, if not addressed adequately, introduce significant risks for the financial institution. The primary challenges are:

- ***Selecting a qualified vendor and structuring the outsourcing arrangement***. The failure to choose a qualified and compatible service provider through an appropriate due diligence process and structure an adequate outsourcing relationship, may lead to ongoing operational problems or even a severe business disruption. The contract should clearly articulate the structure of the outsourcing arrangement and the expectations of both sides, including renewal and termination terms; otherwise, excessive amounts of management time may be consumed with dispute resolution or with managing a contentious relationship.
- ***Managing and monitoring the outsourcing arrangement***. Without active management and monitoring of the relationship, subpar service may occur or, at the extreme, loss of control over the outsourced activity. Even when alternatives are available, switching service providers is likely to be a costly option that adds to operational, legal and reputation risks. The outsourcing contract and internal risk management should ensure that complete and immediate access to critical information is available.
- ***Ensuring effective controls and independent validation***. Given the reliance on a third party for the performance of critical activities, there is a risk that without independent validation of the control environment the savings association cannot determine that the controls have been effectively implemented. A savings association's internal audit function or evaluation by a third-party reviewer can accomplish this. The right of independent validation should be established in the contract.
- ***Ensuring viable contingency planning***. Given the dependency on a third-party service provider, savings associations face the challenge of ensuring adequate contingency planning to avoid business disruptions. Management should verify that the service provider has an adequate contingency plan. Furthermore, savings associations need their own contingency plan in the event of nonperformance by their service provider. The failure to provide for an adequate contingency plan by both the service provider and the savings association may result in unintended financial losses, missed business opportunities and reputation damage.

While a third party provider may be performing the actual functions, it is merely acting as an agent of the trustee and the trustee can still be liable for any mistakes or errors made by its agent. Therefore, if a trust department decides to outsource any operational functions, it must establish a monitoring system for these outsourced functions. The following is a list of items that may require management action or monitoring in an outsourced environment:

- New account information
- Name and address changes
- Fee schedules
- Tickler records
- Initial write up of transactions
- Review of all account data after posting
- Control totals
- Demand deposit account reconciliation
- Daily wire settlement
- Overdraft and excess cash balances
- Affirmation of trades
- Communication on corporate actions
- Income collection for unique assets
- Provide information for nonrecurring checks
- Mail customer reports

Safekeeping and Custody of Assets

Introduction

The operations area is responsible for safeguarding trust assets from the time that they are received until the time those assets are sold, transferred or otherwise delivered out of the trust department. This section discusses procedures and controls that a trust department utilizes to protect its customers' assets.

Section 5(n)(2) of HOLA requires a savings association to "segregate all assets held in any fiduciary capacity from the general assets of the institution". That requirement is implemented by 12 CFR §550.250, which requires the investments of each account to be kept separate from the assets of the savings association and from all other accounts (except when invested in common or collective investment funds). To satisfy this and other safeguarding requirements, basic internal controls that should be present in all departments include:

- ***Dual Control***. As required by 12 CFR §550.230, access to fiduciary account assets should be authorized by at least two designated individuals (defined as officers or employees designated for that purpose either by the board of directors or by a person(s) designated by them). Written procedures should be in place to ensure that dual control procedures are followed in transactions of fiduciary account assets.
- ***Vault Access***. Access to the location where assets are stored should be restricted to authorized personnel. Assets are normally stored in either a separate trust vault or in a separate area of the savings association's main vault. Individuals that access the vault should sign vault logs or other control

records and individuals that control the vault should verify that such personnel are authorized to enter the vault.

- ***Separation of Duties***. A basic concept of internal controls is that control can best be achieved through a separation of duties. No individual should therefore be permitted to both execute and review any transaction. For example, individuals assigned responsibility to execute securities transactions should not be authorized to reconcile daily securities transactions.
- ***Physical Vault Protection Measures***. The vault used for the safekeeping of trust department assets should provide for minimum security devices consistent with the requirements of the Bank Protection Act and related OTS regulations, which provide for (among other things) the installation of appropriate lighting, alarm and other physical security controls. Further information concerning protective measures can be found in the OTS Compliance Activities Handbook, Section 405, Bank Protection Act.
- ***Reconcilements***. Individuals who initiate or authorize transactions or routinely post to the recordkeeping system should not perform reconcilements of deposit accounts, suspense accounts and securities depository statements. In addition, exceptions should be documented and followed up until resolved.
- ***Tickler Systems***. Accurate and timely processing of operational items requires operation personnel's timely attention to nonroutine and nonrecurring tasks. The administration of numerous accounts, each having its own unique servicing requirements, necessitates adoption of a uniform system of control to ensure the timely and accurate performance of these duties. Many institutions implement a tickler system to monitor these activities. A tickler system is nothing more than a chronologically arranged system of records that reminds department employees to collect income, distribute funds and calculate trust fees, etc. Though simple in design and concept, accuracy and effective use of its contents can be critical for account administration.
- ***Other Control Elements***. The organizational structure of a trust department is another component of overall control. Management must define its functional lines of responsibility and establish an organizational framework along those lines. It must then develop logical patterns of workflow. These procedures should take into account the need for checks and balances as well as the need for an efficient, practical system. Control systems should be reviewed regularly and continuously updated. Review of organizational and system controls should be incorporated into the savings association's risk management assessment process. Although they will vary from institution to institution, each control system should encompass the following in some form:

    - Adoption of a comprehensive operations manual
    - Provision for surprise audits (internal and external)
    - Periodic verification of assets held at the institution
    - Daily proof of transactions (balancing and closing routines)
    - Review and signing of transaction journals by administrators
    - Maintenance of accounting records on a current basis
    - Requirements for regular, separate account reconciliation
    - Dual signature requirements for checks over a certain dollar amount

- Requirements for documentation authorizing asset changes, cash distributions and large overdrafts
- Use of prenumbered documents in sequential order
- Audit trails for all accounting transactions
- Proof of records by individuals not authorized to post them
- Review of accounts by individuals other than the administrator assigned to them
- Separate control over checks returned undelivered
- Procedures for reissuance of returned checks
- Adequate record retention policy
- Separated responsibilities for customer statement review and processing

Examiners should recognize that an effective system of policies and procedures designed to establish dual control, duty separation and rotation may be costly. Examiners need to exercise judgment in assessing a department's control system. For example, a system may have one or more deficiencies but the system may be strengthened by reliance upon a strong audit or compliance/quality control review function.

Nominee Registration

Nominee ownership is a means of registering securities in the name of a person, partnership or corporation. Nominee ownership is used to facilitate the management of trust department accounts. When many accounts in a trust department hold shares in the same company, for example, the nominee method makes it easier to sell or transfer securities and to collect interest and dividends. When a securities issuer pays interest or declares a dividend, the institution receives a single dividend or interest payment in the nominee name in which the security is registered. The department then credits the proper accounts holding the particular security, typically using an automated report called a "dividend map." Without the use of nominee registration, separate dividend or interest payments would be received for each account holding the security.

Nearly all states provide by statute that trust department securities may be registered in nominee form and most governing instruments also authorize the department to do so. For the trust department to utilize nominee registration, the board of directors must authorize the execution of a partnership agreement between designated personnel and the institution. This agreement establishes a legal name, which should be registered with the state. Securities held in the trust department can then be registered in the name of that nominee. Examiners should ascertain that the department's nominee partnership agreements are periodically reviewed to ensure that they are current. For example, an examiner should determine whether all of the partners are still with the trust department.

As a rule, the institution should not register securities in the street name of a broker-dealer. An exception to this prohibition may be when the trust department is acting as an agent for investment management services. However, the institution should ensure that any arrangement with a broker-dealer adequately indemnifies the institution from risk of loss or manipulation by the broker.

Securities Lending

Some trust departments are involved in securities lending activities. This is a fee-based service whereby the trust department lends customers' securities held in certain trust department accounts; common and collective investment funds; as well as proprietary mutual funds.

Securities lending primarily occurs in employee benefit plans maintained by large employers. Personal trust accounts and agency accounts are involved to a lesser degree. The primary borrowers of securities are brokers and commercial banks. The securities are borrowed to cover securities fails (securities sold but not delivered), short sales and for option and arbitrage positions. Securities lending is conducted through open-ended agreements that may be terminated on short notice by either the lender or borrower. The objective of such lending is to increase a portfolio's yield beyond the collection of interest and/or dividends.

Securities lending occurring in qualified employee benefit accounts are subject to the Employee Retirement Income Security Act of 1974 (ERISA). Securities lending transactions between a plan and a party in interest would ordinarily be prohibited by ERISA, however, a prohibited transaction class exemption has been issued by the Department of Labor (PTE 81-6) which permits a party in interest to lend securities of employee benefit plans to which it provides services. The exemption contains specific requirements regarding type and amount of collateral, documentation, terms of the loan, compensation and termination of the arrangement.

Some of the restrictions contained in PTE 81-6 are as follows:

- The borrower (or its affiliate) may not have any investment discretion over the plan assets involved in the transaction or render investment advice to the plan.
- The plan receives from the borrower, by the close of the business day on which the securities are delivered to the borrower, collateral consisting of cash, securities issued or guaranteed by the U.S. government or its agencies, or irrevocable bank letters of credit issued by a person other than the borrower (or its affiliate), equal to 100 percent of the market value of the securities lent. Collateral value and market value are to be determined as of the close of business on the preceding business day.
- Prior to any securities lending transaction, the borrower furnishes to the lending entity the most recently available audited statement of the borrower's financial condition (or an unaudited statement if it is more recent) and a representation that, at the time the securities lending transaction is negotiated, that there has been no material adverse change in its financial condition since the date of the most recent financial statement.
- The securities lending transaction is made pursuant to a written agreement the terms of which are at least as favorable to the plan as an arms length transaction with an unrelated party.
- The plan (1) receives a reasonable fee that is related to the value of the borrowed securities and the duration of the transaction or (2) has the opportunity to derive compensation through the investment of the cash collateral.
- The plan receives the equivalent of all distributions made to holders of the borrowed securities during the term of the loan, including, but not limited to cash dividends, interest payments, shares of stock as a result of stock splits and rights to purchase additional securities.
- The market value of the collateral held by the plan must be maintained at 100% of the market value of the securities out on loan.

- The transaction may be terminated by the plan at any time.

Another prohibited transaction class exemption related to securities lending activities of employee benefit plan assets is PTE 82-63. This exemption provides relief from the prohibitions of ERISA Section 406(b)(1) for certain compensation arrangements and also authorizes common and/or collective investment funds in which employee benefit assets are invested, to engage in securities lending transactions. The exemption does not dictate a specific form of compensation but instead merely indicates that the compensation received by the lending fiduciary (i.e. the savings association) must be reasonable and paid in accordance with the terms of a written agreement. Another condition is that the securities lending arrangement must be approved in writing by a plan fiduciary that is independent of the lending fiduciary. The independent plan fiduciary must be able to terminate the arrangement within prescribed time periods without penalty to the plan. The lending fiduciary must also provide the independent plan fiduciary with all reasonably available and necessary information regarding the securities lending arrangement.

For those accounts not governed by ERISA, securities lending activities should be conducted by knowledgeable management, in accordance with written policies and procedures under an adequate system of monitoring and controls. At a minimum, policies and procedures should cover each of the following (See Revised Federal Financial Institutions Examination Council Supervisory Policy, July 21, 1997):

- ***Recordkeeping.*** A recordkeeping system should produce daily reports showing which securities are available for lending; which are currently lent; outstanding loans by borrower; outstanding loans by account; new loans; returns of loaned securities; and transactions by account. These records should be updated as often as necessary to ensure that the lender institution fully accounts for all outstanding loans; that adequate collateral is required and maintained; and that policies and concentration limits are being followed.
- ***Administrative Procedures.*** All securities lent and all securities standing as collateral must be marked to market daily. Procedures must ensure that any necessary calls for additional margin are made on a timely basis. In addition, written procedures should outline how to choose the trust department account that will be the source of lent securities when they are held in more than one account. Security loans should be fairly allocated among all accounts participating in a securities lending program. Internal controls should include operating procedures designed to segregate duties and timely management reporting systems. Periodic internal audits should assess the accuracy of accounting records; the timeliness of management reports; and the lender institution's overall compliance with established policies and procedures.
- ***Credit Analysis and Approval of Borrowers.*** Credit and limit approvals should be based upon a credit analysis of the borrower. Such an analysis should be performed prior to establishing a lending relationship and periodically thereafter. Credit reviews should include an analysis of the borrower's financial statement and any other factors that appear relevant.
- ***Credit and Concentration Limits.*** An individual credit limit should be established for each borrower. That limit should be based on the market value of the securities to be borrowed and should take into account possible temporary (overnight) exposures resulting from a decline in collateral values or from occasional inadvertent delays in transferring collateral.
- ***Collateral Management.*** Security borrowers must pledge and maintain collateral that is at least 100% of the value of the securities borrowed. Excess collateral should be required in cases of volatility of the loaned securities or the nature of the collateral, if other than cash. Generally, the minimum initial

collateral on security loans is at least 102% of the market value of the lent securities, plus, for debt securities, any accrued interest. A daily "mark-to-market" procedure must be in place to ensure that calls for additional collateral are made on a timely basis. Securities should not be lent unless collateral has been received or will be received simultaneously with the loan.

- ***Cash as Collateral.*** When cash is used as collateral, the savings association as lender is responsible for making it income productive. Generally, a savings association will invest cash collateral in repurchase agreements, master notes, a short-term investment fund, U.S. or Eurodollar certificates of deposits, commercial paper or some other type of money market instrument. The written agreement authorizing the lending relationship should specify how cash collateral is to be invested. NOTE: If the cash collateral is invested in a mutual fund, common or collective fund or other pooled fund maintained by the savings association or its affiliate or where the savings association or its affiliate acts as investment adviser, there is a conflict of interest which can be overcome only by specific language in the securities lending agreement or other governing document, state or federal law or court order.
- ***Letters of Credit as Collateral.*** Since May 1982, letters of credit have been permitted as collateral in certain securities lending transactions outlined in Federal Reserve Regulation T. If a lender institution plans to accept letters of credit as collateral, it should establish guidelines for their use. Those guidelines should require a credit analysis of the financial institution issuing the letter of credit before securities are lent against that collateral. Analyses must be periodically updated and reevaluated.
- ***Written Agreements.*** Securities should only be lent pursuant to a written agreement between the savings association as lender and the owner of the securities (generally the plan sponsor) specifically authorizing the savings association to offer the securities for loan. The agreement should outline the savings association's authority to reinvest cash collateral (if any) and its responsibilities with regard to custody and valuation of the collateral. In addition, the agreement should detail the fee or compensation that will go to the savings association in the form of a fee schedule or other specific provision. The savings association as lender must also have written agreements with the parties who wish to borrow securities. These agreements should specify the duties and responsibilities of each party.

Trust departments must also take the following into consideration before engaging in any securities lending transactions:

- Authorization by the governing account instrument or appropriate state law.
- For accounts over which the bank exercises investment discretion, the decision to lend securities represents an investment decision, which should meet the appropriate fiduciary standards. The following considerations should be documented: 1) the appropriateness of the transaction with regards to account objectives and beneficiary needs; 2) diversification; and 3) the prudence of the investment.

Off-Premises Custody

12 CFR §550.240 permits investments of a fiduciary account to be deposited elsewhere to the extent permitted by law. The laws of most states do in fact permit such deposits. Savings associations have increasingly chosen to hold trust department assets in an off-premises depository, such as a national or regional securities depository (for stocks and bonds), a Federal Reserve Bank (for book-entry holding of U.S. Government obligations) or a correspondent institution. For assets held at a depository (or other location), the trust department should ensure that the depository has established adequate controls and safeguards and

that it provides adequate insurance coverage against possible loss or theft. ERISA, in §404(b) contains very strict guidelines regarding the maintenance of the indicia of ownership of any plan asset outside the jurisdiction of the district court of the United States. Regulations issued by the Department of Labor at 29 CFR §2550.404(B-1) do provide some exceptions.

When assets are deposited elsewhere, the trust department should ensure that its own recordkeeping system does the following:

- Records the actual location of each asset
- Reconciles changes in the depository position daily and fully reconciles its position at least monthly
- Provides dual control procedures for the release of securities from the depository
- Ensures that any release of securities directed via telephone, fax or e-mail is properly confirmed
- Ensures that terminal interfaces used to effect withdrawals are subject to appropriate password access controls

Deficiencies in Operations and Controls

Losses and unwarranted exposure due to misappropriation, fraud or embezzlement has in many cases occurred when deficiencies existed in operations or controls. While discovery of such defalcations is not the primary objective of a trust and asset management examination, the examiner should nevertheless be alert to practices that could permit or encourage them.

The following is a partial list of the areas in a trust department that are particularly susceptible to manipulation and abuse. These are merely to be used as examples and are not meant to be an all-inclusive list of the weaknesses that may occur within a savings association's trust operations area. Examiners and trust department management may want to refer to these examples as tools when assessing the controls existing within a savings association's trust operations function. However, management's most effective means of preventing defalcations is a system of comprehensive internal controls and a good audit program.

- ***Failure to record the receipt of assets when accounts are opened***. Detection of a theft is nearly impossible if an asset has never been recorded on the institution's ledgers. The unwitnessed assembling of assets, particularly those of decedents' estates, is a dangerous practice. In such cases, detection of theft may be impossible since no record of a missing asset exists in the savings association's files.
- ***Unauthorized or forged withdrawals of cash and securities from accounts***. Typically caused by the absence of dual controls, this practice involves the manipulator transferring assets to his or her own control, where the assets are then sold, pledged for personal loans or used in market speculation.
- ***Diversion of income on assets received in either irregular amounts or at irregular intervals***. Most often involves diverting income on assets received in either irregular amounts or at irregular intervals (thus making it less likely to detect) out of the trust department's account and into the employee's personal account. Such income is usually derived from royalties, oil wells and the like. Income from all investments should be internally controlled and audited, with added attention given those situations where investments produce income irregularly.

- ***Diversion of stale outstanding checks, inactive deposits and assets of dormant accounts for personal gain***. A combination of independent and timely reconcilement procedures, together with the periodic tracing of transactions from initiation to conclusion can greatly reduce the likelihood of such diversions.
- ***Falsification of expenses and misapplication of commissions and fees***. Expenses and recurring fees present possibilities for manipulation. The savings association should have a policy that requires expenses to be accompanied by appropriate documentation. Individual account administrators should not have control or access to expense checks. Similarly, adequate internal safeguards should exist to assure the crediting of commissions and fees to the appropriate accounts.
- ***Manipulation of payments received on rental properties, real estate and real estate mortgages***. Administration of these trust and asset management account properties frequently involves handling cash payments received in the trust department in person or through the mails. Unless strong internal controls are in effect, defalcations through manipulation of payments could occur.
- ***Improper use of suspense accounts***. Frequently, trust department suspense accounts are not governed by good internal control procedures and unauthorized settlements or disbursements may easily occur.
- ***Misuse of corporate bonds, notes and stock certificates***. Usually occurs where the trust department is holding inventories of unissued securities not under dual control. Securities are stolen, sold or used as collateral for loans.

Improper or illegal securities trading practices

- Placing personal trades through institution accounts, thereby obtaining the advantage of the savings association's volume discounts on commissions;
- Purchasing or selling an issue of securities prior to executing trust and asset management account trades which could be expected to change the price of the security, thereby obtaining a personal price advantage ("front-running");
- Purchasing and selling the same securities issue on the same day, with the trader pocketing any price increases and assigning transactions to trust and asset management accounts in the event of any price decreases; and
- Buying or selling based on nonpublic material inside information that might affect the price of the securities, thereby enabling the trader to benefit personally from the transaction. This is a violation of securities laws that should be reported to the Securities and Exchange Commission (SEC).

Securities Processing Systems and Controls

The operations area is responsible for the processing of securities and other assets. (For convenience, the term "securities" is used in this section to refer to trust department assets). Securities processing includes both the physical movement of securities through the department (i.e., from the vault through the processing or trading area, through settlement and out of the department) and the controls in effect over that movement. Specifically, the securities processing area is responsible for securities trading and settlement activities involving:

- receipt of authorization and instruction for a securities trade (purchase or sale);
- placement of the trade with a broker or trading desk for execution;
- reconcilement of in-house trade information to broker's confirmation received subsequent to trade execution;
- receipt or delivery of securities against payment; and
- posting of the trade to the affected account.

Any operations function, regardless of the department's size, must devise a system for monitoring and controlling the movement of securities and the processing of daily and periodic transactions and withdrawals. Many institutions have designed and implemented formal security movement and control systems. The objective of such systems, commonly referred to as "SMAC" systems, is to detail all asset movements. A manual SMAC system utilizes manually prepared security tickets for the purpose of monitoring and controlling security movement activities. Automated SMAC systems improve the control over and monitoring of security activities through system-generated management and/or exception reports that are available daily or on demand. One of the principal benefits of an automated SMAC system is its ability to reference, extract and post to an automated recordkeeping system. Therefore, such systems are either incorporated within an automated recordkeeping system or are designed as independent systems with the capability (system interface) of accomplishing these benefits.

Regardless of the formality with which such systems are utilized in a particular department, the control aspects of these systems should include:

- written acknowledgment by joint custodians;
- date of all vault transactions;
- description of securities;
- identity of the affected account; and
- information regarding the transaction, including, for example, the source of the securities being deposited and the purpose for which securities are being withdrawn.

Trade Orders and Executions

Purchase or sale orders for accounts can, depending on the savings association's investment responsibility, be initiated from the trust department's authorized investment personnel, from customers or from outside investment advisors or managers. When received, such orders should be documented on order tickets or similar records and should include the account for which the order is to be executed; a full description of the security; the time the order was received by the trader; the time the order was placed with the broker; the unit and aggregate price at which the order was executed; the broker utilized; and whether or not the transaction is subject to any special instructions. Those records should be maintained in a manner that provides a chronological record of all daily activity. In the past, many departments utilized prenumbered multi-part forms that monitor an individual trade from beginning to end. However, this process is increasingly giving way to electronic tracking of trade orders.

One of the fundamental duties of a fiduciary is to seek the best execution for its customers when trading securities. While this is not strictly an operations function, the operations area can nevertheless provide input into this determination by providing information as to the timeliness and accuracy of trade execution and settlement services provided by the broker, any commission discounts given and the broker's ability to handle block trades.

Confirmation, Settlement and Posting

Brokers are required to provide written confirmation to the department following notification of execution. The confirmation should include the full details of the trade and be reconciled to the original trade memoranda by a person independent of the person who placed the trade. Similarly, the department should send a copy of the confirmation to the customer, detailing the transaction and including any fees charged to the account. Generally accepted fiduciary principles, SEC rules as well as those of the other bank regulatory agencies (12 CFR Part 12) provide certain confirmation requirements. For example, the time, form and content of the confirmation or notification is prescribed as well as the circumstances under which a customer can waive his or her right to receive the confirmation.

Settlement occurs when securities are exchanged for cash payment. The date of settlement is generally set at three business days after execution of the trade (T + 3) but may vary by agreement between the institution and the broker or the type of security being traded. Any position that remains open past settlement date should be subject to written procedures.

Securities trades are posted in one of two ways. Under the first, referred to as contractual settlement date accounting, the customer's account is posted on the contractual settlement date specified on the trade confirmation, regardless of whether or not the security is actually received. An offsetting entry for payment is made to a separate suspense account for purchases and sales. That entry is cleared when the securities are actually received and payment is made. Under the second, referred to as actual settlement date accounting, the customer's account is posted on the actual date of settlement. Most automated accounting systems enter pending trade notifications to customers' accounts when trades are executed and do not make offsetting cash entries until actual settlement occurs. These systems also monitor open trades by producing daily reports listing trades open past settlement date.

Receipts and Disbursements

The securities processing unit is responsible for the collection of receipts payable on trust department assets such as dividends, interest, rents, royalties and other cash and noncash payments. Income may be received on either a regular basis, such as bond interest, or an irregular basis, such as royalties on mineral interests. In either case the department should have a tickler or similar system to monitor the receipt of all income to ensure that it is received when due. Such tickler systems can range from a card index that details fixed income payments and serves as a reminder on irregular ones (found in smaller, nonautomated departments) to a system-generated report of anticipated income (found in automated departments). An automated system will usually credit the appropriate accounts with the income due, once the payment is received.

Over or underpayments of income should be posted to a suspense account or otherwise earmarked as due, pending further research. Funds received as overpayments should be held pending a documented claim from the rightful owner. In the absence of a claim and if a certain amount of time passes (usually seven years, but state law should be consulted), the department is required to comply with state laws regarding escheatable or unclaimed funds. In the case of pension assets subject to ERISA, the examiner should note that the

Department of Labor has taken the position in many advisory opinion letters that pension plan assets may never be escheated to a state.

When the department has not received full payment, established procedures should be followed to determine the reason for the underpayment and a written claim against the appropriate party should be filed.

All requests for disbursements, whether for cash, securities or other assets, should follow established procedures. While the form and content of acceptable procedures may vary, they should at least provide that disbursements will be made only upon written request to authorized personnel and that receipts should be obtained.

Miscellaneous Trust Department Operational Activities

Introduction

An additional function of trust operations and sound internal controls is to ensure compliance with management policies, applicable law and established fiduciary principles. While the previous sections focused on systems and procedures as they relate to overall trust department operations, this section focuses on the role that trust operations plays in ensuring compliance when the trust department engages in certain activities.

Cash Management - Uninvested Cash

Trust and asset management accounts often receive cash in the form of receipts (dividend and interest payments) or contributions. These accounts may need cash in order to make required distributions and to pay expenses. Thus, it is rare that an account will have all of its assets invested all of the time. On the other hand, 12 CFR §550.290 requires that fiduciary funds, where the savings association has investment discretion or discretion over distributions, that are awaiting investment or distribution, are not to be held uninvested or undistributed any longer than is reasonable for the proper management of the account. Section §550.300 provides that any funds awaiting investment or distribution may be deposited in other departments of the savings association, unless prohibited by applicable law. Both sections require that fiduciary funds so invested must obtain a rate of return that is consistent with applicable law. These regulations essentially codify the common law responsibility to make trust property productive. Fiduciaries have been held liable for failing to invest cash within an appropriate period of time. In these circumstances the fiduciary has been surcharged for the earnings that could have been obtained had the funds been properly invested.

In order to satisfy the standard set forth in §550.290 and to demonstrate compliance with a fiduciary's common law duty to make trust property productive, a trust department should have an effective and efficient cash management system. Such a system should:

- minimize the dollar amount and length of time that income and principal cash is left uninvested in an account; and
- place available cash, on a daily basis, into short-term vehicles that return a reasonable rate of interest.

The application of these regulations must necessarily be based upon a review of all the facts and circumstances relevant to each savings association and to each affected account. However, to ensure

compliance and to avoid possible surcharge, the department should have written policies and procedures to govern the management of cash in fiduciary accounts and should utilize cash management systems and techniques. The decision to leave any cash uninvested in fiduciary accounts should be supported and documented in the trust department's records.

A cash management vehicle should be able to provide a high degree of liquidity and safety. Examples include short-term time deposits; U.S. Treasury bills; commercial paper; money market funds; short-term investment funds; deposit accounts; and corporate variable amount or master notes. The investment vehicle used for cash management purposes must be prudently selected and any conflict of interest overcome by appropriate state law, document language or court order.

Some savings associations have historically placed uninvested funds in a savings account. However, given the number of alternative cash management vehicles available in the current financial environment, it would be exceedingly difficult to justify holding a large cash balance in a savings account. Similarly, some savings associations historically utilized a zero interest time deposit open account (TDOA) for trust account cash. According to the Federal Reserve Board, (in a letter dated May 17, 1991 to the OCC) it was general practice not to pay interest on these accounts. For the reasons noted above, generally restated in the Fed's letter, this practice should be viewed as inconsistent with basic fiduciary responsibilities and sound trust department administration.

Cash Sweep Fees

Savings associations are increasingly utilizing automated accounting systems to provide cash management programs. Under these "cash sweep" systems, uninvested cash and/or available cash balances are automatically swept into one or more short-term vehicles of the type described above. In a nonautomated department, acceptable and effective cash management practices may consist of placing the funds in a money market deposit account or mutual fund.

A department's cash sweep service for fiduciary accounts where the savings association has investment discretion may raise questions in addition to those discussed above if a separate fee is involved, either directly or indirectly. The practice of sweeping fiduciary account cash and receiving a separate fee for this service has been the subject of litigation in various courts. The separate fee issue has not been decided, as of yet, by any U.S. Appellate courts. The one case that had reached that level was dismissed on jurisdictional grounds. As a result, the question of whether a fiduciary may charge an additional or extra fee for its cash sweep service depends upon the law in a particular state or the specific language in the governing document. The following guidelines may be applied to discretionary fiduciary accounts where a separate fee is charged in connection with cash sweep services:

- An initial determination should be made as to whether the fee is specifically permitted by state law or permitted under the terms of the governing instrument.
- If state law specifically permits the fee, then no further inquiry need be made except in terms of determining compliance with any of the statutory restrictions. The same reasoning applies in connection with authorization language in the governing document.
- If state law or the governing instrument does not specifically permit the fee, the institution should obtain a reasoned opinion of counsel that addresses the permissibility of the fee, including any requirements relating to authorization, consent and/or disclosure.

- If state law permits "reasonable" fees, the department should consider the extent to which such a sweep fee may be charged as well as what authorizations, consents, and/or disclosures should be obtained or provided.
- If the fiduciary's compensation is fixed by statute or in the governing instrument, then all parties affected by a change must consent to the change. An opinion of counsel should be obtained to ascertain how consent may be obtained for minor beneficiaries, unknown or unborn beneficiaries.
- Imposition of a sweep fee for accounts in which a savings association has investment discretion may also raise conflict of interest questions, depending on the investment vehicle utilized in the sweep arrangement. If the investment vehicle is a proprietary mutual fund or a mutual fund in which the savings association receives direct or indirect compensation, a specific state statute, language in the governing instrument or a court order must be in place permitting the use of the mutual fund.
- With respect to this practice for employee benefit accounts subject to ERISA, a department should be encouraged to seek the prior advice of the Department of Labor or have a reasoned opinion of counsel that considers the sweep service in relation to ERISA's prohibited transaction provisions. The DOL has indicated in Advisory Opinion 88-02A (February 2, 1988) that such sweep services will not violate 406(a), 406(b)(1)(2) or (3) of ERISA provided that the institution does not have investment discretion over the plan assets and that an independent investment advisor determines whether and how much uninvested cash will be swept and chooses which of several money market funds will be utilized. An independent third party sponsored all of the funds in question. Another condition is that the bank, in this case, did not receive a fee or other compensation for any of the money market funds involved in the sweep program. Another condition that the DOL notes is that the plan must be notified no less than 30 days prior to any change in the fees to be charged for the service and that the arrangement is subject to immediate termination without penalty.

Revocable trust accounts where the savings association does not have full investment discretion and custodial trust accounts may be charged a separate fee for sweeping services provided appropriate disclosure is made and there are no prohibitions in either state law or in the governing instrument.

Overdrafts

Overdrafts occur when more income or principal cash is disbursed than exists in a particular account. Overdrafts can result from problems that arise due to differences in settlement cycles, cash distributions that must be made in accordance with the governing instrument without sufficient liquid assets in the account or from other causes. Overdrafts in general should be temporary in nature, made only for proper purposes and be reflected on account records. Policies and procedures should be in effect to govern the department's treatment of overdrafts and to ensure that they are appropriately monitored and kept to a minimum.

Overdrafts can be placed into two distinct categories.

The first category is of less concern because overdrafts are permitted by the terms of the governing instrument and there are no separate income and principal beneficiaries, or the separation of income and principal cash is primarily for tax purposes. In these instances assets shown in the income column, for example, offset a temporary shortage in the principal column. Overdrafts in estates, guardianships and agency accounts generally fall into this category.

In the second category, cash balances in the income column for example, cannot offset a net overdraft in the principal column. This represents a potential liability to the trust department. In most personal trust accounts, the separation of income and principal cash is important because the income and principal beneficiaries may be different persons. Since the trustee may not favor one class of beneficiaries over another, the general rule is that income and principal cash cannot be netted against each other in order to show a combined positive balance. Thus, for example, if the department advances funds to an income beneficiary, thereby overdrawing income cash, and if the income beneficiary dies, the department would have to reimburse the account. In addition, if a trust department improperly nets trust account overdrafts from demand balances held in another department of the savings association, it may be understating its reserve requirements, and therefore in violation of the Federal Reserve Board's Regulation D (see the Thrift Activities Handbook, section 561, reserve requirements). Overdrafts are also a concern when they occur in a custodial account that is actively engaged in the buying and selling of securities without sufficient cash. In these situations, free riding may be taking place. (Refer to the section on free riding if overdrafts are shown for custodial accounts).

For nonfiduciary accounts, such as custodial accounts, savings associations typically charge a rate of interest against the account when the savings association covers overdrafts and the overdraft has occurred as a result of a situation beyond the control of the savings association. Overdraft policies and rates should be disclosed at the beginning of a customer relationship so that customers understand the terms of overdraft coverage. Overdraft rates are generally set at a level expected to provide a reasonable rate of return on the bank's capital and to discourage overdrafts from occurring unnecessarily.

Overdrafts in employee benefit accounts typically occur when savings associations, acting as a trustee or custodian, receive trading instructions from nonaffiliated investment managers of the plan before a prior trade has settled. Although the vast majority of securities transactions settle on time, settlement problems may arise due to unexpected delays, miscommunication, errors or inefficient foreign market practices. It is often operationally impossible, given time constraints, for savings associations to reconcile the cash flows in employee benefit accounts before each transaction clears, instead the settlement process runs continuously. At the end of the day, the accounts are reconciled. If the reconciliation shows that a particular account had insufficient funds when a trade was settled, an overdraft has occurred. The savings association typically covers these overdrafts with its own funds. There is a prohibited transaction class exemption (PTE 80-26), which permits a party in interest to make interest free loans (the payment of the overdraft is considered by the DOL to be a loan) to an employee benefit plan. The party in interest is the savings association. The proceeds of the loan may be used only for certain purposes one of which is to cover temporary overdrafts by a plan trustee to pay for securities or the crediting of dividends or interest by a bank trustee prior to receipt of such dividends or interest. Under the exemption, no interest or other fee may be charged by the savings association to the plan for the payment of the overdraft. Other conditions are that the overdraft may not occur longer than three days and the loan may not be secured.

Consumer Lending Activities

A trust department, on behalf of a trust and asset management account or on behalf of a private banking client, may engage in activities covered by consumer protection laws and regulations. These activities normally arise where the trust department is granting or purchasing loans as a form of investment or in connection with the sale of real estate that is an asset of an account. In some cases, such as under the Truth in Lending Act and its implementing Regulation Z, the consumer protection laws would apply because the trust department is considered to be a "creditor." Under Regulation Z, a person or organization is considered a creditor, and therefore subject to Regulation Z, if it extends consumer credit more than 25 times in the

preceding calendar year or more than 5 times for transactions secured by a dwelling. Each individual account and its trustee (i.e., the savings association) are considered a single (separate) entity for purposes of determining whether it is a creditor.

When the trust department is acting as trustee or recordkeeper for an employee benefit plan, it may be responsible, on behalf of the plan, for complying with Regulation Z disclosures in connection with employee benefit plan loans to plan participants. An employee benefit plan is deemed to be a creditor for Truth in Lending purposes if it regularly extends consumer credit that is payable in more than four installments, or for which the payment of a finance charge is or may be required, and if it is the party shown as the payee on the face of the note evidencing the loan. Truth in Lending requires a plan fiduciary as a creditor to make disclosures to the borrowing participant with respect to certain credit information, including: 1) interest rates; 2) finance charges; 3) amounts financed; 4) payment schedules; 5) demand features; 6) prepayment penalties; 7) late payment fees; and 8) security interest descriptions. The plan must disclose other relevant credit information so that the borrowing participant can compare the various credit terms available to him from different sources. Regulation Z contains extensive guidance as to which fees are considered finance charges, the calculation of finance charges and requirements applicable to open-end credit and closed-end credit. Most, if not all, plan loans will be deemed to be closed-end credit and subject to the Truth in Lending requirements applicable to such credit. A loan over $25,000, not secured by real property or the borrower's principal dwelling is exempted from Truth in Lending requirements. Thus, larger plan loans will be excluded from complying with the disclosure requirements.

In extending credit or dealing in residential real estate investments, a trust department may also be subject to the disclosure requirements of the Real Estate Settlement Procedures Act (RESPA) as well as the laws and regulations related to fair housing and fair lending. The review of these real estate related activities would normally come within the scope of a compliance examination. If that examination is being conducted separately from a trust and asset management examination, appropriate regional area office personnel should be notified of the existence of any of these activities occurring in the trust department.

The trust and asset management examination should determine whether consumer protection compliance considerations are included in trust department policies and procedures, and if no such considerations are apparent, management should be advised to assess the department's possible exposure under the various statutes.

Bank Secrecy Act

The fundamental purpose of The Currency and Foreign Transactions Reporting Act, also known as the Bank Secrecy Act is to provide a paper trail of the activities of money launderers serving the interests of drug traffickers and other elements of white collar and organized crime. To this end, the Act was enacted to discourage the use of currency in illegal transactions and to identify and report unusual or questionable transactions. The requirements of the Act apply to all activities, products and services offered by a savings association's trust and asset management and private banking departments. The BSA requirements typically come into play in regards to wire transfers.

The Bank Secrecy Act regulations (31 CFR §103) require all financial institutions to submit five types of reports to the government whenever certain situations occur. OTS regulations regarding the suspicious activity reports and other reports and statements under the BSA are located at §563.180. Some of the reports that may be applicable to trust department activities are listed below.

- ***IRS Form 4789 Currency Transaction Report (CTR):*** A CTR must be filed for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through or to a financial institution, which involves a transaction in currency of more than $10,000. Multiple currency transactions must be treated as a single transaction if the financial institution has knowledge that: (a) they are conducted by or on behalf of the same person; and, (b) they result in cash received or disbursed by the financial institution of more than $10,000.
- ***Treasury Department Form 90-22.47 Suspicious Activity Report (SAR):*** Financial institutions must file a SAR for any suspicious transaction relevant to a possible violation of law or regulation.

Financial institutions are also required under the BSA regulations to maintain a variety of records to ensure, among other things, that transactions can be reconstructed. The retention period for all records required to be kept under the BSA regulations is five years. One of the records that trust departments may be required to keep is:

- ***Funds Transfer Recordkeeping and Travel Rule Requirements:*** A financial institution must maintain a record of each fund transfer of $3,000 or more which it originates, acts as an intermediary for or receives funds transfers. The amount and type of information a bank must record and keep depends upon its role in the funds transfer process. Also, a savings association that acts as an originator or intermediary for a funds transfer must pass certain information along to the next bank in the fund transfer chain.

OTS at 12 CFR §563.177 requires savings associations to establish and maintain procedures reasonably designed to assure and monitor compliance with the recordkeeping and reporting requirements established by the Bank Secrecy Act. The BSA compliance program is required to be reduced to writing, approved by the board of directors and reflected in the minutes of the savings association. The compliance program, at a minimum, must: 1) provide for a system of internal controls to assure ongoing compliance; 2) provide for independent testing for compliance to be conducted by a savings association's in-house personnel or an outside party; 3) designate individual(s) responsible for coordinating and monitoring day-to-day compliance; and 4) provide training for appropriate personnel.

Shareholders Communications Act

The Shareholders Communications Act of 1985 gave the SEC authority to regulate the proxy processing activities of banks and all other entities exercising fiduciary powers. This includes savings associations' trust departments that hold securities in nominee name or otherwise on behalf of beneficial owners. SEC Rule 14b-2, which is promulgated under the Securities Exchange Act of 1934, implements the Act. The rules govern the distribution of proxy materials to, and the disclosure of identifying information about, shareholders whose securities are registered in a nominee name. Note that the beneficial owner, for purposes of these shareholder communications rules, is not necessarily the person who owns the security or receives the dividends. For example, a savings association that has the authority, as fiduciary for a trust account, to vote the securities held in the account is deemed the beneficial owner under the rules. Similarly, if an investment manager (savings association) has been assigned the right to vote securities on behalf of a customer, the investment manager (and not the customer) is the beneficial owner, for purposes of this rule.

Essentially, the Rule stipulates that financial institutions must comply with certain requirements to facilitate communications between issuers of registered securities ("registrants") and the holders of those securities ("beneficial owners"). The requirements address proxy distribution procedures and provisions regarding the disclosure of beneficial owner information.

There are several phases in the proxy distribution procedures under Rule 14b-2. Financial institutions are required under the rules to respond to search card requests from the issuers of registered securities (i.e. the corporation or the mutual fund company) to determine beneficial owners in order to send proxies, annual reports and related materials. The financial institution then will distribute the proxy material to their customers, seeking voting instructions from them. Upon receipt of these voting instructions, the financial institution communicates the results to the corporation or the mutual fund company. An exception to these rules applies to employee benefit plans whose participants have pass-through voting powers (Rule 14b-2(c)).

Self-Directed IRA's

Under 12 CFR §550.580, a savings association does not need trust powers to act in a fiduciary capacity regarding certain types of accounts. These accounts include Individual Retirement Accounts within the meaning of Internal Revenue Code 408(a). Under this section, a savings association may act as a trustee or custodian of these accounts (without trust powers) if the IRAs are invested in the savings association's accounts, deposit obligations or securities or other assets as the customer directs. The savings association, may not (without trust powers), in regard to these accounts, offer investment advice or exercise any investment discretion.

Despite the fact that institutions are permitted, within the constraints of state law, to offer these products without trust powers, the accounts are considered fiduciary accounts. The institution is required to treat them as it would any other fiduciary account. In addition, the administration of these accounts must also comply with, as applicable, the Internal Revenue Code, ERISA and state law.

Where savings associations with trust powers offer or provide services to these accounts within the trust department, the accounts and related practices should be reviewed during trust and asset management examinations. Where institutions that do not operate a trust department offer these products, the institution's practices should be reviewed as part of the nondeposit investment products review segment of the safety and soundness or compliance examination. Additional information and guidance are provided in the examination procedures for nondeposit investment products.

Examiners should ensure that sufficient documentation exists to adequately identify and support each account. The assets of these IRAs should be accounted for separately from the savings associations' own assets. The institution's internal audit coverage should include this activity.

Free Riding

"Free riding" generally involves individuals trading large amounts of securities without depositing the necessary money or appropriate collateral in their customer accounts. The customer seeks to free ride that is, purchase and sell the same securities and pay for the purchase with the proceeds of the sale. Targeted investigations in the early 1990s by the Enforcement Division of the Securities and Exchange Commission found banks in violation of Regulation U in connection with extensions of credit (overdrafts) by bank trust departments, using bank or other fiduciary funds, to individuals involved in illegal "day trading" or "free-riding" schemes. Banks were also found to be aiding and abetting violations of two other securities credit regulations: Regulation T and Regulation X.

If the money to pay for the securities is not in the account when the securities are delivered in a delivery-versus-payment (DVP) or receive-versus-payment transaction, a savings association that permits completion of the transaction creates a temporary overdraft in the customer's account. This overdraft is an extension of

credit that is subject to Regulation U. Regulation U includes a requirement that all extensions of credit that are secured by marginable stock be within the 50 percent margin limit set by Regulation U. Savings association involved in free-riding schemes may be aiding and abetting broker-dealer violations of Regulation T. Regulation T applies to broker-dealers only and it requires the use of a cash account when a customer purchases or sells securities on a DVP basis. If a savings association uses its funds to complete a customer's transactions, the broker-dealers may not discover that they are selling securities to the customer in violation of their obligations under Regulation T. Regulation X is also involved in these schemes as this Regulation generally prohibits borrowers from willfully causing credit to be extended in contravention of Regulations T or U.

Free riding often begins when a custodial account is opened with a trust department. The customer also establishes brokerage accounts through which the customer directs securities trades. The customer then advises the broker-dealer that payment for such trades will be made through the custodial account. The perpetrator attempts to profit from short-term changes in market prices of securities, without placing significant personal funds at risk. Free riders frequently place a buy order for securities, anticipating a near-term price increase and intend to pay for the securities with the proceeds from the sale of the same securities.

At a minimum, examiners should evaluate a trust department's ability to ensure that it does not extend more credit on behalf of the banking organization to a customer than is permitted under Regulation U. Any overdraft related to a purchase or sale of margin stock is an extension of credit subject to the regulation, including overdrafts that are outstanding for less than a day. Examiners should also make sure that savings associations follow appropriate written policies and procedures concerning the establishment of custodial agency accounts or any new account involving customer securities transactions. Such policies and procedures should:

- Set standards for the acceptance of new custodial accounts, including customer background, credit information and a determination of whether the customer will be obtaining bank credit to use the account as if it were a margin account. The institution should inquire, if the customer has indicated that it will be obtaining bank credit, why the customer is not utilizing the margin account services of its broker-dealer. If the account is to be used as a margin account, Regulation U Form FR G-1 must be obtained and constantly updated.
- Require identification of the broker-dealers that will be sending securities to and receiving funds from the account on a DVP basis. The institution should establish systems to track accounts involving numerous broker-dealers.

The institution should require, as part of its account agreement that the customer will take responsibility to make sure that all account transactions with broker-dealers will be in conformance with Regulations T and X.

State Escheatment Laws

Escheat is defined as a reversion of property to the state in consequence of the lack of any individual qualified to inherit the property. In trust departments the issue will generally arise concerning unassigned dividend or interest payments; bond coupons not presented for payment; bonds not presented for payment; uncashed employee benefit plan participant distribution checks; and certain suspense account assets. Trust departments acting as bond trustees, securities transfer agents, and paying agents should consult state abandoned property laws for: (1) checks and securities certificates which are undeliverable and (2) book-entry accounts for which the owner cannot be located. Escheat laws vary from one state to another. They

will normally be found in state statutes under titles such as "unclaimed property" or "abandoned property." In some instances, one state may claim its escheat laws apply to dormant funds also claimed by another state.

It is important that the trust operations area have some procedure in place to assure compliance with these laws. Examiners should familiarize themselves with relevant state law on the issue of escheatment and be alert during examinations to qualifying stale items and other instances where such law might be applicable.

Examiners should note that outstanding checks issued by an employee benefit plan for distribution to plan participants or for other purposes, are, according to the Department of Labor, never subject to state escheatment laws. The Department of Labor takes the position that outstanding checks represent plan assets that can never be escheated. The DOL has claimed preemption over state escheatment laws in a number of advisory opinions issued over the years.

Pledge Requirements

12 CFR §550.310 requires that trust funds on deposit with the institution or an affiliate awaiting investment or distribution must be fully collateralized if they are in excess of FDIC insurance coverage. The types of acceptable collateral for uninsured deposits are detailed in 12 CFR §550.320. This requirement pertains to all deposits of fiduciary account assets with the institution or an affiliate, including demand deposit accounts, certificates of deposit, money market deposit accounts and savings accounts. The institution should adopt and implement procedures, which ensure the periodic review of the adequacy of any collateral pledged in accordance with these regulations.

To illustrate, the calculation of collateral for a single account with a single beneficiary involves adding the account's net demand deposit balance; any outstanding checks drawn on that balance; any funds awaiting investment or distribution deposited in interest-bearing accounts (as opposed to invested funds); and any funds of the account held in suspense or other in-house accounts. The totals of all individual accounts in excess of insurance limits can then be added together to determine the minimum necessary collateral for a particular day.

Custodial Holdings of Government Securities

A succession of highly publicized failures of government securities broker-dealers that caused large losses to investors occurred from the mid-1970s to the mid-1980s (e.g., Drysdale, Lombard-Wall, E.S.M.). As a result of these failures and improper practices, Congress exercised its authority over the largely unregulated government securities market through passage of the Government Securities Act of 1986 (GSA). The stated purpose of the GSA and its implementing regulations is to enhance the protection of investors in government securities by establishing and enforcing appropriate financial responsibility and custodial standards.

The GSA applies to all financial institutions that engage in government securities activities. For the purposes of the GSA, government securities include:

- U.S. Treasury bills, bonds and notes;
- Discount notes, bonds, certain collateralized mortgage obligations, pass-throughs, master notes, obligations of the Government National Mortgage Association (GNMA), the Federal National Mortgage Association (FNMA), the Federal Home Loan Mortgage Corporation (FHLMC), the Student Loan Marketing Association (SLMA), the Farm Credit System (FCS) and the Financing Corporation; and

- FNMA or FHLMC stock.

"Off-exchange" puts, calls, straddles and "similar privileges" on government securities are considered to be government securities except for the rules addressing custodial holding of securities.

The GSA requirements impact savings associations (referred to in the law and regulations as financial or depository institutions) in three main areas:

- Savings institutions that are government securities brokers or dealers are required to file a notice with the Office of Thrift Supervision of their status as such by the date of their becoming a government securities broker or dealer and to comply with applicable requirements relating to those activities.
- Savings institutions that engage in repurchase transactions with customers while retaining custody or control of government securities ("hold-in-custody" repurchase transactions) must comply with requirements relating to written agreements, confirmations and disclosures.
- Savings institutions that hold government securities for customers, as fiduciary, custodian or otherwise, must comply with requirements relating to the safeguarding and custody of those securities (17 CFR §403.5). The GSA regulation applies whether an institution holds the customers' securities directly or maintains the customers' securities through another institution. A "customer" is any party for whom the institution maintains government securities.

This handbook section covers the holding of government securities in fiduciary or custodial accounts. More information on the other requirements under the Government Securities Act is covered in Section 563 of the Thrift Activities Handbook.

The regulations at 17 CFR §403.5 note that there is an exemption at 17 CFR §450.3 regarding the holding of government securities in fiduciary accounts. This exemption only applies to banks, not savings associations regulated by the OTS. Until such time as that exemption becomes available to savings association, savings associations must comply with the requirements contained in Part 450 of the GSA regulations.

References below are to the applicable GSA regulations.

Possession and Control Requirements (450.4(a))

All government securities held for customers must be (1) segregated from the savings association's own assets and (2) kept free of any lien or other claim by a third-party granted or created by the savings association. For securities maintained for the savings association at another depository institution ("custodian institution), compliance of the above requirement is achieved if: the savings association notifies the custodian institution that such securities are customer securities; the custodian institution maintains the securities in an account that is designated for customers of the savings association and that account does not contain any securities belonging to the savings association itself; and the savings association instructs the custodian institution to maintain the securities free of any lien, charge or claim of any kind in favor of the custodial institution.

Thus, if a savings association is maintaining both custodial and fiduciary customers' securities and its own securities at a custodial institution, it must have at least two accounts at the custodial institution: one for holding custodial and fiduciary customers' securities and one containing its proprietary securities.

Notwithstanding the possession and control requirements, a savings association may lend securities to a third party pursuant to the written agreement of the customer if such loan complies with the supervisory guidelines of the OTS.

Confirmation Requirements (450.4(b))

A confirmation or safekeeping receipt must be issued to a customer for each government security held. The confirmation or safekeeping receipt must identify the issuer, maturity date, par amount and coupon rate of the security being confirmed. A savings association shall not be required to send the confirmation or safekeeping receipt to a customer that is a non-U.S. citizen residing outside the U.S. or a foreign corporation, partnership, or trust, if such customer expressly waives in writing the right to receive such confirmation or safekeeping receipt.

Recordkeeping Requirements (450.4(c)-(f))

A records system of government securities held for customers must be maintained separate and distinct from other records of the savings association. These records must (1) identify each customer and each security held; (2) describe the customer's interest in the security (i.e., "subject to repurchase agreement" or "pledged to secure a public deposit"); and (3) indicate all receipts and deliveries of securities and cash in connection with the securities. A copy of the safekeeping receipt or confirmation given to customers also must be maintained and the system of records must provide an adequate basis for audit. Finally, the required records must be maintained in an easily accessible place for at least two years and not disposed of for at least six years.

Verification Requirements (450.4(d))

A savings association is required to conduct a count of physical securities and securities held in book-entry form at least annually. An annual reconcilement with customer account records must also be performed. The savings association responsible for the count must verify any securities in transfer, in transit, pledged, loaned, borrowed, deposited, etc. when the securities have been out of the savings association's possession for longer than 30 days. The dates and results of the counts and reconcilements must be documented within seven days of the required count with any differences noted.

Securities Subject to Repurchase Agreement (403.5(d))

All financial institutions that retain custody of securities sold under an agreement to repurchase must comply with the requirements for hold-in-custody repurchase agreements. If the customer agrees to allow substitution of securities in a hold-in-custody repurchase transaction, then authority for the savings association to substitute securities must be contained in the written repurchase agreement. In all hold-in-custody repurchase agreements where the savings association reserves the right to substitute securities, a specific disclosure statement must be prominently displayed in the written repurchase agreement immediately preceding the provision allowing the right to substitution. A savings association must disclose to the customer in writing that the funds held pursuant to the repurchase agreement is not a deposit and therefore not federally insured. Written confirmations describing the specific securities subject to the transaction must be sent to the customer by close of business on the day the transaction is initiated, as well as on any day on which a substitution of securities occurs. In addition to the specific information discussed above under "confirmation requirements," confirmations must include the market value (defined as the most recently available bid price for the security, plus accrued interest) and CUSIP or mortgage pool number of

the underlying securities (unless identified in internal records of the broker-dealer). Finally, pooling of securities, as collateral for repurchase agreements are no longer permitted.

CHAPTER: Operations, Internal Controls, Audit and Information Technology

SECTION: Operations & Internal Controls Examination Program — Section 310P

Examination Objective

To determine the adequacy and/or effectiveness of the trust department's operations and internal controls. Consider whether:

- all transactions are executed in accordance with applicable law and fiduciary principles;
- there is adequate documentation and timely execution of all transactions;
- the trust department has adopted and implemented an effective system of policies, procedures and practices;
- all accounting, custody, control and security processing systems and records are checked for reliability;
- segregation, custody and control are in accordance with applicable law, policies and procedures; and
- deficiencies are identified and corrective action is initiated as necessary.

Examination Procedures

Level I Level I procedures first focus on a review of the examination scoping materials. The next step consists of interviews with trust department personnel to confirm their qualifications and levels of expertise; to determine if the trust department's practices conform to written guidelines; to establish whether any significant changes in personnel, operations or business practices have occurred; or whether new products and/or services have been introduced. If items of concern are uncovered during Level I procedures or if problems are identified during the preexamination monitoring and scoping, the examiner may need to perform particular Level II procedures.

1. Review examination scoping materials related to the trust department's operations and internal controls. Scoping material should include:

   - Risk profile
   - Relevant PERK documents
   - Previous trust and asset management examination report
   - Workpapers from the previous examination
   - Safety and soundness examination report
   - Examination reports of subordinate, functionally regulated entities
   - Board of director and/or appropriate committee minutes

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

- Web site information

[Click&type]

2. Evaluate the operations and internal control policies and procedures regarding:

   - compliance with applicable law and fiduciary principles;
   - the reliability of the systems and records for accounting, safekeeping, custody and securities processing; and
   - exception transactions.

[Click&type]

3. Evaluate whether management has the expertise necessary to carry out the operations and internal control policies and procedures.

[Click&type]

4. Determine any significant changes in policies, procedures or outsourcing arrangements.

[Click&type]

5. Determine whether management monitors outsourcing arrangements, e.g. through a review of SAS 70 reports and committee minutes.

[Click&type]

6. Review and evaluate any significant personnel and/or organizational changes.

[Click&type]

7. Determine whether any new trust or asset management products or service have been instituted.

[Click&type]

8. Evaluate management's procedures for monitoring the savings association's web site. If transactional, was the proper OTS notification and approval obtained?

[Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

9. Consider whether the following risk contributors (if applicable) have been addressed:

- Does management fully understand all aspects of operational risk?
- Does management anticipate and respond well to market and technological changes?
- Is the volume and complexity of transactions supported by the current system(s) and system development initiatives?
- Is the internal control environment strong so the trust department is not exposed to transaction failures? Are there adequate controls over outsourcing arrangements?
- Do management information reports satisfactorily monitor transaction processing?
- Does management quickly identify weaknesses and take appropriate action?
- Are there any unresolved operational issues noted in the audit, compliance or examination report(s)?
- Does management adequately budget for system maintenance and for software and hardware needs?
- Are there adequate disaster recovery plans?

[Click&type]

The completion of the Level I procedures may provide sufficient information to make a determination that no further examination procedures are necessary. If no determination can be made, proceed to Level II.

Level II Level II procedures focus on an analysis of trust department documents such as reports and outsourcing contracts. The examiner should complete the appropriate Level II procedures when the completion of Level I procedures does not reveal adequate information on which to base a conclusion that the trust department meets the examination objectives. Neither the Level I nor the Level II procedures include any significant verification procedures

1. Determine whether internal controls are adequately monitored. Consider such items as:

- safekeeping of unissued trust checks;
- controlling computer access to accounting records;
- separating duties for the authorization, signing and mailing of trust department checks;
- handling and distributing trust account statements;
- separating duties for input, processing and reconcilement of trust account information;

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

- verifying and safeguarding trust and estate personal property;
- confirming after posting that the aggregate of debits and credits posted to the system agree with posting totals generated by the system;
- determining whether the savings association controls and monitors the use of facsimile signature devices;
- the proper receiving, holding or withdrawing of securities, other assets or unissued checks in and out of the vault; and
- determining whether the savings association follows proper cash management practices.

[Click&type]

2. Determine whether individual account ledgers are balanced against the trust department's general ledger on a regular basis. Consider whether internal accounts are reconciled regularly and exceptions are timely cleared.

[Click&type]

3. Determine if the trust accounting system generates sufficient and reliable information regarding each trust department account. Consider whether the following reports are regularly generated and reviewed by appropriate personnel:

- overdrafts;
- excess cash;
- issued and outstanding checks;
- investment transactions;
- asset classification; and
- principal and income posting.

[Click&type]

4. Determine if there are adequate dual control procedures for trust account assets held for safekeeping in the trust department vault.

[Click&type]

5. Determine whether proper monitoring and controls exist regarding the movement of securities and the processing of daily and periodic transactions and withdrawals. Consider whether there are system-

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

generated management and/or exception reports available. Also consider whether such a manual or automated system includes:

- a written acknowledgement by joint custodians;
- dated vault transactions;
- description of securities;
- identity of the affected account; and
- information regarding the transaction, including, for example, the source of the securities being deposited and the purpose for which securities are being withdrawn.

[Click&type]

6. Determine if adequate controls exist regarding purchase or sale orders for trust department accounts. Consider whether there is adequate documentation regarding directions provided by outside investment managers.

[Click&type]

7. Determine if there is adequate documentation regarding the execution of the purchase or sale order.

[Click&type]

8. Determine if policies and procedures are adequate to determine if broker confirmations are reconciled against the savings association's securities transaction register.

[Click&type]

9. Determine if the trust department monitors the receipt of soft dollars and brokerage commissions being charged.

[Click&type]

10. Determine whether there is correct usage and adequate monitoring by management of suspense and overdraft accounts.

[Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

11. Determine whether the securities processing unit has adequate controls regarding:

    - obtaining and disbursing accurate information regarding corporate reorganizations, puts, calls and tender offers;
    - posting and collecting all dividend and interest payments;
    - obtaining prior approval to settle particular security trades; and
    - validity and accuracy of wire transfers.

    [Click&type]

12. Determine if trust funds on deposit with the savings association or its affiliate are secured in accordance with OTS regulations at §550.290-320.

    [Click&type]

13. Determine when investment discretion has been delegated to an outside or affiliated investment adviser(s). Ensure that recommendations and/or decisions are appropriate for the affected trust department accounts in accordance with applicable state law requirements.

    [Click&type]

14. Determine if the trust department's controls and safeguards for its securities lending activities are adequate.

    [Click&type]

15. Determine if the trust department has proper controls in place to prevent "free riding".

    [Click&type]

16. Determine if the trust department has adequate policies and procedures to govern its obligations in connection with the Shareholder Communications Act and proxy processing regulations.

    [Click&type]

17. Determine if the trust department has adequate policies and procedures to comply with state escheat laws.

    [Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

18. Review compliance monitoring procedures for any transactional web site.

[Click&type]

If the examiner cannot rely on the trust and asset management Level I or Level II procedures, or data contained in department records or internal or external audit reports; proceed to Level III.

Level III Level III procedures include verification procedures that auditors usually perform. Although certain situations may require that Level III procedures be completed, it is not the standard practice of the Office of Thrift Supervision (OTS) examination staff to duplicate or substitute the testing performed by auditors.

1. Reconcile individual account ledger totals to the trust department's general ledger.

[Click&type]

2. Test the accuracy of purchase and sale transactions by comparing selected broker confirmation statements to the securities transaction register.

[Click&type]

3. Test for timely posting of items to selected trust accounts. Ensure that postings to income and principal are correct.

[Click&type]

4. Reconcile trust department demand account balances to outstanding trust department checks.

[Click&type]

5. Test selected trust department customer account statements for accuracy.

[Click&type]

6. Reconcile suspense accounts.

[Click&type]

7. Review all exception reports and verify resolution.

[Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Final Risk Assessment

Determine a final risk assessment regarding the trust department's operation and internal control environment based on the level of examination conducted.

Type of Risk	Quantity of Risk: High, Medium, Low	Quality of Controls: Effective, Acceptable or Weak	Direction of Risk: Increasing, Decreasing or Stable
Reputation Risk			
Strategic Risk			
Transaction/Operational Risk			
Compliance/Legal Risk			
Financial Risk			

Support the ratings from the matrix above with a concise summary explanation for each of the risk categories as to quantity, quality and direction of risk.

Overall Risk Assessment
[Click&type]

Examiner's UITRS Rating, Summary, Conclusions and Recommendations:

[Click&type]

References - 310

Laws

HOLA	Section 5(n)(2)
ERISA	Section 404(b)
	Section 406(b)
Share Holders Communication Act	
Bank Secrecy Act	
Internal Revenue Code	Section 408(a)

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Code of Federal Regulations

12 CFR 550.230	Custody or Control of Assets in a Fiduciary Account
12 CFR 550.240	Custody of Fiduciary Investments on Off-site Premises
12 CFR 550.250	Segregation of Fiduciary Assets
12 CFR 550.290	Funds Awaiting Investment or Distribution
12 CFR 550.300	Deposit of Temporary Investments
12 CFR 550.310	Pledging for Deposits
12 CFR 550.320	Acceptable Collateral
12 CFR 550.430	Fiduciary Records Separate and Distinct
12 CFR 550.490	Deposit of Securities with State Authorities
12 CFR 550.510	Records
12 CFR 550.580	Exempt Activities
12 CFR 563.117	Bank Secrecy Act Procedures
12 CFR 568	Minimum Security Devises and Procedures
17 CFR 403.5	Custody of Securities Held by Financial Institutions that are Government Securities Brokers or Dealers
17 CFR 450.4	Custodial Holdings of Government Securities
29 CFR 2550.404(b)(1)	Maintenance of Plan Assets Outside of Jurisdiction of US Courts
31 CFR 103	Bank Secrecy Act Regulations

Office of Thrift Supervision Publications

OTS Compliance Activities Handbook	Section 405

Other

PTE 81-6	Securities Lending from Qualified Plans
PTE 82-63	Payment to Fiduciaries for Providing Securities Lending Services
DOL Advisory Opinion 88-02A	Sweep Fees
SEC Rule 14a	Shareholders Communication Act

Workpaper Attachments - 310

[Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Optional Topic Questions

The following list of questions is offered merely as a tool and reference for the examiner and is not a required part of the examination process.

Policies, Procedures and Records

- Has the savings association adopted a formal disaster recovery and contingency plan?
- Are account records posted daily?
- Are entry source documents initiated by an individual not responsible for posting the entry to the accounting system?
- Are individual account cash and asset ledgers sufficiently clear to identify transactions, current holdings and balances?
- Are there trust departmental control accounts that provide accounting control over all assets?
- Are trial balances generated periodically?
- Are there regular reconcilements of trust department demand account balances and outstanding trust checks?
- Are separate ledger controls for each account maintained for principal and income?
- Is there use of departmental (general ledger) accounts to ensure that accounting control is provided over all assets?
- Are there accurate and complete asset and transaction descriptions?
- Are postings to the system once a source document is received, done timely?
- Is confirmation after posting done to ensure that the aggregate of debits and credits posted to the system agree with posted totals generated by the automated system?
- Does the savings association's system have the ability to generate information (or reports) for the following key controls?
  - Aged breaks (identify breaks between trust accounting and other systems)
  - Asset classification (separate assets by type)
  - Automatic investment of dividends
  - Overdraft report
  - Excess cash report
  - Transaction report of previous day's activity
  - Income receivable reconciliation
  - Issued and outstanding checks
  - Daily checks

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Account Statement Processing

• Is there a verification or quality control for statements regarding cash balance reconciliation, asset pricing, verification of pending trade settlement dates, transaction detail, loan detail or fee charges?
• Does the savings association have a controlled environment for the processing (including changes) and review of statements prior to mailing?

Suspense Accounts

• Are all suspense or "house" accounts identified?
• Is there a periodic reconcilement of all suspense accounts?
• Does the frequency of reconcilement depend on the number and/or dollar amount of transactions?
• Are suspense accounts used only for the purpose intended?
• Does an individual who is not authorized to generate or post entries to the account, reconcile suspense accounts?
• Are exceptions documented and followed up on a timely basis until they are cleared?
• Is the time period an exception is outstanding noted? Are exceptions outstanding for 30-60 days reported to senior management? Are exceptions outstanding for a certain time (usually 90 days) being charged off to the savings association if no recovery within a reasonable time is foreseen?
• Are exception reports reviewed and initialed by a supervisor?

Outsourcing Arrangements

• Did management perform an adequate due diligence review of the service provider?
• Is there a contract with the service provider that clearly articulates the expectations and responsibilities of both sides? Does the agreement include a clause whereby the savings association may rescind the agreement if the service provider is not adequately performing?
• Is there an effective structure in place to manage and monitor the outsourcing arrangement?
• Has management ensured that the service provider has a viable contingency plan?
• Does management obtain and review audit/examination reports (such as a SAS 70) of the service provider?
• Does the savings association have complete and immediate access to critical information?

Trust department vault

• Is there a separate trust vault or lock box for trust assets in the savings association's main vault?
• Is the vault under dual control (at least 2 personnel authorized to enter the vault)?
• Does the board of directors or their designee appoint vault custodians?
• Is a written log denoting time of entry, who entered and what was taken or placed in the vault, maintained?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Nominee Registration

• If trust securities are held at the Depository Trust Company (DTC) in the nominee name of CEDE & CO, is there a written agreement and are the authorized signers for the savings association added or deleted on a timely basis?
• If another nominee name is utilized, is it registered with The American Society of Corporate Secretaries (to guard against duplication of the nominee name) or the appropriate state authority if so required?

Control of Assets

• Are trust assets properly secured at all times?
• Are transactions processed on a timely basis?
• Is there timely follow-up to update asset values for proper pricing as to both market and cost values?
• Are securities being handled in a secured area with limited access?
• Is there use of prenumbered receipt or withdrawal forms or fanfold tickets for the deposit or withdrawal of assets? Are these deposits or withdrawals verified and authenticated in writing by joint custodians?
• Are trust department checks prepared and disbursed by someone other than the person who authorized them?

• Are there proper physical controls of unissued trust department checks to prevent unauthorized issuance? This should include:
  • Checks being prenumbered;
  • Checks being used in numerical order;
  • Periodic reviews should be performed to make sure no checks are missing; and
  • Working supply signed out (in a log) and stored in locked desk or cabinet when not in use.

• Are changes to customer records initiated by appropriate parties and supported by adequate documentation?
• Are unissued checks and unissued securities of corporate trusts and transfer agencies held in the vault along with records of those withdrawn?

Custodial Holdings of Government Securities

• If the savings association holds securities for the account of a customer (including securities subject to repurchase transactions) does it maintain possession and control by:
  • Segregating such securities from the assets of the savings association?
  • Keeping them free of any lien, charge or claim of any third party granted or created by the savings association?

• If customer securities are maintained at another financial institution (a “custodian” financial institution such as a correspondent bank but other than a Federal Reserve Bank), does the savings association:
  • Notify the custodian institution that such securities are customer securities?
  • Instruct the custodian institution to maintain such securities free of any lien, charge, or claim of any kind in favor of the savings association or any persons claiming through it?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

- Receive adequate assurance from the custodial financial institution that securities are being maintained in an account designated for the savings association's customers and such account does not contain proprietary securities of the custodian financial institution or the savings association?

- Where the savings association is holding securities for another financial institution as a custodian, does it:
  - Receive notification from the depositing financial institution regarding which securities are customer securities?
  - Maintain such customer securities free of any lien, charge or claim of any third party granted or created by the financial institution?
  - Treat such securities as customer securities and maintain such securities separate from any other securities held for the account of the depositing financial institution, and from any other securities held by the savings association?

- If the savings association is providing clearing services for a government securities broker or dealer by holding securities that have been identified as customer securities by such broker or dealer, does the savings association:
  - Treat such securities as customer securities separate from other securities held for the account of the broker or dealer; and
  - Comply with the same requirements detailed above when the customer securities are maintained at another financial institution; or
  - If the securities are not segregated as of the close of business upon the broker-dealer's instruction, does the savings association have procedures for giving notification to the supervising agency of the broker or dealer that such securities are not being segregated because they continue to be required as collateral for an extension of clearing credit to such dealer and are such procedures being followed?

- If customer securities are maintained for the savings association at a Federal Reserve Bank, does the savings association have procedures designed to prevent the unauthorized pledge of customer securities to the Federal Reserve Bank?

- Review the savings association's procedures for complying with the regulation regarding the issuance of a confirmation or a safekeeping receipt for each security held.
  - Does the confirmation or safekeeping receipt identify the issuer, the maturity and the par amount and coupon rate of the security?
  - Is the confirmation supplied to the customer in the manner specified in the regulations?

- Review the savings association's compliance with the recordkeeping requirements of 17 CFR 450.4(c) and determine if the savings association's records:
  - Provide a system for identifying each customer and each security?
  - Describe the customer's interest in the security?
  - Indicate all receipts and disbursements of securities?
  - Indicate all receipts and disbursements of cash by the savings association in connection with government securities?
  - Include a copy of the safekeeping receipt or a confirmation issued for each security held?

- Review the policies and procedures for securities held for customers (17 CFR 450.4(d)) and determine if:
  - Policies and procedures are adequately documented.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

• Actual counts are performed at least annually. • Securities are reconciled with customer account records. • Securities held by another institution, as custodian, are properly reconciled. • Securities that have not been in the savings association's possession for longer than 30 days are verified, including those in transfer, transit, pledged, loaned, borrowed, deposited, failed to receive or deliver, subject to repurchase or reverse repurchase agreements?
• Review the savings association's policies and procedures for complying with government securities that are subject to a repurchase transaction. 17 CFR 403.5(d): • Are written agreements between the customer and the savings association on file? • Does the repurchase agreement state that the funds held by the savings association are not a deposit and therefore not federally insured? • If the right to substitute securities is granted the savings association, does the repurchase agreement contain a provision allowing it to substitute securities? • Is the savings association in compliance with the substitution provision?

Securities Lending

• Has management developed and implemented adequate written policies, procedures and a system of controls that will enable the trust department to conform to applicable law as well as minimize the potential risks associated with securities lending?
• Is there authorization contained in the governing instrument?
• Is the activity subject to a written agreement between the security borrower and the savings association delineating duties of each (custodianship of collateral, collateral margin, types of securities to be used as collateral, default procedures, etc.)?
• Does the savings association have personnel who are knowledgeable and experienced in securities lending?
• Is a due diligence analysis and review of the borrower periodically updated?

Free Riding

• Are the policies and procedures adequately documented?
• Have standards been set for the acceptance of new custodial accounts, including customer background and credit information?
• Is identification required of broker-dealers sending securities to, and receiving funds from, customer accounts?
• Has a system been established to track accounts involving numerous broker-dealers?
• Is it policy to disaffirm customer trades where acceptance would result in a violation of Regulation U?
• Are procedures in place to determine that if margin credit is extended, that collateral requirements are met?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Introduction to Audits

This section provides guidelines to evaluate a trust department's audit program and to evaluate the work performed by internal and external auditors. Many of the considerations used to evaluate a trust department's audit program are the same as those used to evaluate the savings association's overall audit, although a separate trust department audit should be conducted. Due to the fact that the trust department may be audited at the same time as the savings association itself, in some regions examiners (other than trust and asset management examiners) may evaluate such matters as the auditor's independence and competence for the institution as a whole. In these cases, the examiner evaluation should separately consider the independence and competence of the auditors with regards to the trust department.

The primary objective of the audit function in the trust department is to detect errors and irregularities and ascertain the effectiveness of the policies and procedures used for the administration of accounts, safeguarding of assets and the accurate recording of transactions.

12 CFR §550.440 requires that a savings association must conduct a suitable audit of its significant fiduciary activities. The regulation permits the savings association to conduct these audits on either an *annual* basis or on a *continuous* basis. If the institution chooses to use an annual audit system it must "arrange for a suitable audit of all significant fiduciary activities at least once during each calendar year" (§440(a)). On the other hand, if the savings association adopts a continuous audit system, it must "arrange for a discrete audit of each significant fiduciary activity at an interval commensurate with the nature and risk of that activity" (§440(b)). Therefore, under this type of audit system, some fiduciary activities may receive audits at intervals greater or less than one year, as deemed appropriate for the risks associated with that activity. For institutions on a continuous audit system, examiners should ensure that a risk assessment has been made for all significant fiduciary activities and that those activities reviewed less often than annually have been determined to be low risk.

Independent audits enhance the probability that conditions that could adversely affect the savings association, OTS or the public will be detected. The audit process also subjects the policies, procedures, records and the internal controls of each institution to periodic review.

Examiners should evaluate a savings association's audit program for its trust department based on a review and evaluation of the competence and independence of the audit staff and the adequacy and effectiveness of the audit program. Areas that would normally be subject to criticism include the absence of an audit function; an inadequate audit program; instances where audit staff is restricted from full access to records or otherwise lacks independence; lack of competence; instances in which the audit function does not report directly to the board of directors (or an appropriately designated committee); and instances where the board or its designated committee is not properly established or initiating necessary corrective action based on audit findings.

Materials that pertain to overall audit policies and standards are noted in more detail in sections 350 and 355 of the Thrift Activities Handbook. Only a brief summary of those materials is presented in this handbook chapter.

Audit Committee

12 CFR §550.470 provides savings associations with guidance as to the composition of the board of director's fiduciary audit committee. Under the regulation, a fiduciary audit committee directs the conduct of the audit. The composition of the committee may consist of a committee of the savings association directors, an audit committee of an affiliate or the entire institution's board of directors. However, the regulation places the following two restrictions on who may serve on the committee:

- savings association officers or officers of an affiliate who participate significantly in administering fiduciary activities may not serve on the committee; and
- a majority of the members of the audit committee may not serve on any board committee responsible for the savings association's administration of its fiduciary activities.

Results of fiduciary audits (including significant actions taken as a result of the audit) must be reported in the minutes of the board of directors.

Trust Department Audit Objectives

The objectives of a trust department audit should be:

- to appraise the soundness and adequacy of accounting, operating and administrative controls and procedures designed to insure prompt, efficient and accurate recording of transactions and safekeeping of assets.
- to determine the degree of compliance with applicable law as well as the institution's policies, practices and procedures.
- to keep the board of directors and management informed of the institution's condition and make recommendations for improvement.
- to evaluate the institution's exposure to liability if the institution fails to fulfill its duties and responsibilities to trust and asset management accounts.
- to detect and prevent irregularities such as errors and fraud.
- to determine the quality of account administration.
- to verify that fee income from trust and asset management activities is recognized properly on the savings association's financial statements.

Examiners should ensure the trust audit function is effective in evaluating the department's internal controls and is of sufficient scope and coverage to protect the interests of trust and asset management accounts and the institution. Examiners should also ensure that the auditors review for compliance with applicable law. The review and evaluation of the audit function should be a key element in determining the scope of the trust and asset management examination. The examiner should generally not duplicate satisfactorily performed audit procedures, particularly those involving verification activities.

Audit reports should provide the examiner with information pertinent to the trust and asset management examination, such as areas where weaknesses were noted and areas where the examiner should determine whether management appropriately corrected cited deficiencies. If the examiner determines that audits have not been performed or that audit work is considered to be of limited value, the examiner should expand the

scope of the trust and asset management examination. In those instances, the audit or audit program and lack of board oversight should be criticized.

Internal and External Audits

In order to satisfy the requirements of §550.460, internal or external auditors, or a combination of both may perform a trust department audit, and should be responsible only to the savings association's board of directors. The form of audit developed and the personnel employed to conduct it will be primarily dependent upon the size and complexity of the trust and asset management activities. The scope and objectives of an external audit may differ somewhat from those of an internal audit. An external audit is generally aimed at enabling the accountant to express an opinion on the fair presentation of financial statements in conformity with generally accepted accounting principles. To that end, the audit requirements subject the accounting policies, procedures, records and the internal controls of each institution to periodic, independent critical review and evaluation and typically cover only a specified historical period.

On the other hand, the internal audit function has a number of objectives, including the detection of errors; determination of compliance with an institution's policies, procedures and applicable law; and evaluation of the soundness and adequacy of an savings association's system of internal controls. Internal auditors may also play a role in the formation and revision of policies and procedures.

Actual practice may blur the distinctions between an internal and external audit. For example, internal and external auditors may work together on the same audit and set the audit scope and assign each auditor an area of responsibility or they may work side by side. Any distinction between internal and external audits is therefore relevant only to the extent that it impacts the quality and effectiveness of a savings association's overall audit program.

If the trust department is audited internally, the examiner should take the opportunity to review the auditor's programs, workpapers and reports as part of the overall examination process. However, if the department is audited externally the opportunity to review programs and workpapers may not always be feasible. In order to adequately assess the work performed by the external auditor, and to address the matters discussed in the preceding paragraph, the external audit report should provide adequate details concerning the areas audited (testing for receipt of income from investments, allocations of income and principal cash, etc.). A statement to the effect that "all applicable audit procedures were performed in compliance with PA-7a," without further elaboration, would not be acceptable. Examiners should encourage management to contact the external auditor and enable examiner access to audit programs and workpapers.

Competence and Independence

(The Thrift Activities Handbook contains detailed information on the competence and independence of auditors; only a brief summary is presented here.)

Two of the major considerations in evaluating the work of auditors are their competence and independence. This evaluation is the same as it would be for evaluating any audit or auditor; the fact that it is a trust department audit makes no difference. Thus, when a trust and asset management examination is being conducted as part of an examination of the entire savings association, an examiner (other than a trust and asset management examiner) may perform the audit evaluation of the trust department.

The very nature of an internal audit requires that it be independent. Only by being independent can the audit function fulfill its purpose of serving as a managerial control within an organization, i.e. to measure and

evaluate the effectiveness of operations and controls. To be independent means that the audit function should report only to the board of directors or its designated committee. The auditor should have full and free access to all books and records. Auditors should not audit any activity for which they are responsible on a daily basis; for example, auditors should not evaluate vault procedures if they are the vault custodians.

The size and complexity of a savings association's trust and asset management activities as well as the emphasis placed on the audit function by the board of directors will account for variations in the responsibilities and qualifications of internal auditors. In considering the qualifications of the audit staff, it is necessary to review the educational and experience qualifications required by the savings association for a position in the audit department and any available training. The trust department auditor must possess sufficient education and training to fully understand trust and asset management administration, investment practices and trust department operations. If a savings association has a small trust department, it may not always be feasible for its auditor to have trust department auditing experience. However, in those cases the auditor should participate in courses or programs sponsored by industry groups dealing with trust department audits and should review current literature on trust department auditing.

Conclusions in regard to the auditor's competence should be derived from a review of the audit program, training and the quality of reports. Indicators of the competence of the internal auditor include the quality of the work performed and the ability to communicate the results to the board.

The independence of the external audit function is similarly critical to the satisfactory performance of audit activities: external auditors must be independent of those for whom they work. The AICPA and OTS have promulgated standards of independence. OTS provides that a public accountant will not be considered independent if, among other things, the accountant or his or her firm has any direct or material financial interest in the savings association. A financial interest is defined as the CPA being connected with the savings association, subsidiary or affiliate as an officer or director; being the beneficial owner of any shares of stock of the savings association; or having any conflict of interest by reason of business or personal relationships with management or other individuals. Absent unusual circumstances, it should not be necessary to review the independence of the external auditor.

Qualified public accountants are required to perform their work according to generally accepted auditing standards. Absent unusual circumstances, it should not be necessary to review the qualifications of the external auditor. Where a review is considered necessary, the above standards relating to specialized work experience would be appropriate.

Audit Program

A savings association should develop a written audit program approved by its board or audit committee. The program should be tailored to the institution's trust and asset management activities; the risks associated with those activities; the experience level of the audit staff; and define an acceptable scope and frequency schedule for the audit. The scope and frequency of the audit testing should be dependent on the degree of risk that the trust and asset management activities pose to the savings association. Riskier activities should be audited more frequently, while those activities posing a minimal risk to the savings association may be tested on a more infrequent basis.

In the case of an external audit, a written program usually consists of having the external auditor submit an engagement letter to the directors prior to beginning their work. Engagement letters typically include the scope of the audit, the time period for the audit, and the reports expected to be rendered. The auditor may also provide a summary of procedures to be used, for example, in the verification of account assets. In the

case of an internal audit, a written program usually consists of a board resolution or an adopted procedure similar to an engagement letter.

The scope of the audit program must be broad enough to include all significant operations and functions of the trust department; however, its focus should be on the activities or operations of the trust department that have been associated with a high level of risk.

To illustrate, the scope of the audit program should consider the:

- past performance or results of past audits.
- organizational structure of the trust department.
- size and complexity of trust and asset management activities (dollar value of assets, level of discretionary accounts, complexity of assets, etc.).
- nature and extent of comments in OTS trust and asset management examination reports.
- individual factors, such as: effectiveness of internal controls, strength and integrity of trust department accounting, recordkeeping and other systems.
- nature and extent of insurance coverage.

Regulatory requirements for the scope of external and internal audits include, among other things, that:

- the audit be made in accordance with generally accepted auditing standards.
- the auditor be generally familiar with applicable law such as appropriate federal and state statutes and OTS regulations (e.g., 12 CFR §550).
- the audit incorporate all procedures necessary to satisfy the auditor that fiduciary activities are being administered in accordance with applicable law, fiduciary assets are being properly safeguarded and transactions are being recorded in appropriate accounts in a timely manner.

Audit Controls

The audit of a trust department can be divided into three main areas: compliance, physical control and activity control. Compliance consists of the prompt and complete fulfillment of all duties required by applicable law and management policies. Physical control includes the physical security of assets for which the trust department is responsible. Activity control includes the complete, accurate and timely recording of all individual account and departmental transactions.

The auditor's primary responsibility in auditing internal controls is to determine that such controls are in place, that the controls address all of the trust department's duties regarding trust and asset management accounts and that the department is in compliance with the internal controls. In terms of physical controls, the audit procedures employed will be determined at least, in part, by the extent to which the department's systems are automated or are otherwise controlled internally. For example, the auditor may perform more actual verification procedures in an automated department so as to determine whether the reconciliation of balances and statements are being properly performed by the internal accounting system, whereas in a nonautomated department the auditor may perform more actual reconciliation of account balances and controls.

An audit should include a review of the organizations that provide services to the department. Such a review will most likely be conducted by reviewing the service provider's own audit report. Such reports are rendered by the servicer pursuant to Statement on Accounting Standards (SAS) 70, which should discuss the control structure in place for trust department service providers, such as data processing servicers and securities custodians. The institution's auditors most likely will be preparing similar SAS 70 reports for use by other auditors, such as a plan sponsor's auditor and also for the trust department's common and collective investment funds.

Audits of Common Procedures and Administrative Audits

An effective trust department audit should include tests of systems and procedures that are common to the management of all or most accounts being administered, as well as tests of activity in individual accounts. Functions that are normally tested are the opening and closing of accounts; processing of assets into and out of the vault; fee charges and payments; and processing of asset purchases and sales.

Testing of individual account activity is referred to as an "administrative audit." In performing administrative audits, the auditor should perform sufficiently detailed tests to obtain reasonable assurance that activities and transactions within the various types of accounts are being conducted properly. A representative sample of accounts should therefore be selected for testing of individual transactions. The approach taken in a particular audit program will determine which functions are tested as part of common procedures and which functions are tested individually as part of an administrative audit. For example, a test of uninvested cash could be performed as a common procedure by obtaining a listing of all such cash or it could be performed as an individual account procedure.

In reviewing the savings association's internal audit program, the examiner should expect to find the following minimum functions being performed:

- Review of trust department committee minutes
- Balance and proof of subsidiary ledgers to general ledger
- Review of broker confirmations
- Spot-check and tracing of transactions for accuracy and validity
- Verification of commission and fee calculations
- Assessment of compliance with applicable law
- Evaluation of internal controls
- An administrative review of selected accounts comprising:
    - The trust agreement, other governing documents and court orders
    - Administrative actions (in compliance with above)
    - Income postings
    - Discretionary distributions
    - Principal invasions (including approvals therefore)
    - Investments in accordance with account objectives and department policy
    - Account documentation

- Consultation with, and approvals by, cofiduciaries

Audit Records and Reports

In order to have a sound basis upon which to evaluate the adequacy of the internal audit program, the audit workpapers must document the work performed by the auditor. Workpapers should contain audit work programs and analysis that clearly indicate the procedures performed, the extent of testing and the basis for the conclusions reached. In addition, the content of the workpapers is one indicator of an auditor's competence and adherence to professional standards. An analysis of the reporting process followed by the auditor and of the findings and recommendations in the audit reports is important in determining the auditor's duties and the independence of the audit function.

Audit reports should be submitted as soon as practicable after completion of the audit. Reports should be sent to those officials who have both the responsibility and the authority to implement the suggested changes. Management's prompt and effective response to the auditor's recommendations is essential to the effectiveness of the audit program. The examiner should determine not only what was contained in the auditor's reports but also the timeliness and content of management's response. The examiner should expect to see either corrective action taken in response to the audit findings or reasons for nonimplementation.

Risk Based Audits

Risk based audit programs are a relatively recent development in the trust and asset management activities arena and are being more widely adopted by trust departments. The primary objectives for implementing a risk-based audit program are to improve the effectiveness of internal audit activity and enhance company profitability through efficient resource utilization. Risk-based auditing programs are designed to place audit resources in the areas of highest risk and enable an efficient and proactive risk assessment and control environment. This process necessitates and fosters cooperation and improved relationships between auditors and management.

Numerous large financial institutions have implemented trust department risk-based auditing programs as part of a corporate-wide, risk-based auditing system. Institution or holding company audit personnel that report to a trust department audit committee of the board typically administer these audit programs. This committee may report to another board audit committee or directly to the board.

Risk-based auditing programs are designed to be dynamic processes that focus on the identification and measurement of risk and the implementation of appropriate risk management systems. It requires, at a minimum, periodic risk assessments of all significant trust and asset management activities. These assessments are documented, reviewed and updated before a new audit of a specific activity has begun. While these audit programs and risk assessment models are primarily internally designed, there are a few vendors who are providing prototype shells, which the financial institution purchases and modifies to meet its particular needs.

The basic design standards of the risk-based auditing programs are similar. There are, however, significant variances in the risk assessment models and monitoring formats. The sophistication of each program will vary with the size, complexity, geographic diversity and technological capital of each financial institution. In designing the program and its components the auditors may work closely with trust department management in order to identify the various trust and asset management products and services and the risks associated with them.

The following is a brief summary of some steps that can be used to begin building an effective risk-based audit program.

- Develop an auditable universe and define auditable entities.

  The first step in the risk assessment process is to develop an auditable universe. Auditors should determine the significant trust and asset management activities of the organization and construct these activities into definable auditable entities. Auditable entities are most often established by business line but are also created by service or function.

- Develop an auditable entity business profile.

  A profile of each trust and asset management auditable entity is then developed that documents the entity's business goals and objectives, strategies, organizational structure and operating systems. The purpose of the profile is to identify key risks inherent in the entity and document the structure of risk management and internal control systems. Workflow analysis is sometimes performed at this stage, but is more frequently documented during the planning of actual audit work programs.

- Prepare the auditable entity risk assessment.

  The trust and asset management risk assessment format is typically structured to evaluate and measure business, inherent risk and control system risk. Within each of these categories, specific trust and asset management risk factors are listed for analysis and provided with a rating (usually numerical). The factors are supported by written standards with definitions and application guidelines. Risk factors vary in focus and number but examples of common factors include the following:

  - financial indicators such as account size and types, transaction volumes, growth trends and earnings;
  - control environment that includes the corporate risk culture, management style and organizational structure;
  - risk management and internal control systems;
  - management information systems and technology;
  - strategic factors such as product development and marketing focus; and
  - compliance, litigation and regulatory environment.

Some trust and asset management risk based audit programs have structured their risk assessment models to specifically address the nine risk categories that have been identified and promulgated by OTS.

Trust and asset management risk based systems may attempt to quantify the various risks through the application of a qualitative model rating system. The risk factors are often rated or scored based on a formalized scale such as High, Medium, or Low, or 1 through 5. Some systems may even apply a weighting factor to the process, which may be based upon the auditor's knowledge of the savings association's history versus industry averages or standards.

Programs may include the use of risk matrixes and charts that compare the risk and control aspects and then attempt to identify control or efficiency gaps. This type of analysis illustrates where business risk is equal to or different from the appropriate risk control level. This "gap" analysis concept is informally applied in the auditor's evaluation of risk and control systems. The matrixes and charts rarely stand on their own. Usually there is a narrative commentary accompanying the matrixes, which analyze and support the auditor's conclusions.

- Develop the trust and asset management risk-based auditing plan.

  Once the risk assessment process is completed, the auditor is now ready to develop his audit plan. The assessment process is used as the primary tool in developing the plan. The audit plan is a comprehensive document that is approved each year by the trust department audit committee or board. It establishes audit schedules, work program scope and resource allocations for each auditable entity.

- Audit execution, exception reporting and follow-up processes.

  Implementation of the trust department audit plan involves three key processes, planning, execution and reporting. During the planning stage, the auditable entity's risk profile is analyzed and a risk-based audit work program is developed which will be used to execute the audit of the specific activities. The auditing process will identify any exceptions found. In the reporting process, the auditor must determine what exception items are reportable in a formalized report and which are communicated to department management in an informal manner.

  Similar to the Uniform Trust Interagency Rating System used by OTS and the other banking regulators, each audit report may contain a rating, categorizing the auditor's overall findings regarding the auditable activity. An activity's overall rating will usually depend upon the amount and severity of exceptions found. The distribution of formalized audit reports may be impacted by the audit report rating with more critical reports receiving broader and higher level distribution.

  Once the report is distributed, the auditor must set up a system to monitor any actions taken by department management to resolve the auditor's concerns. The exception rating system may also impact the timing of the auditor's follow-up of audit exceptions. The follow-up program should require some form of monitoring for all exceptions regardless of their significance.

- Implement systems to monitor and update risk assessments.

  Prior to the next audit, the risk assessments will need to be reviewed and updated to reflect any changes from the last audit.

  Formally or informally, trust department auditors are provided periodic monitoring information reports for risk assessment purposes. The auditors use the information to adjust auditing priorities but an update of the risk assessment profile or matrix of the trust department may or may not be completed until the required annual assessment date or until an audit is conducted.

- Audits of One or More Affiliates

  With the continual growth in multi-bank and unitary thrift holding companies, many financial organizations now have one or more of its subsidiaries performing trust and asset management activities. Many of these holding companies will use their holding company internal auditors to perform audits of their subsidiaries' trust and asset management activities. In order to create efficiencies, many of these auditors will perform an audit of a specific function or functions for each of the trust and asset management subsidiaries at the same time rather than auditing a subsidiary institution's entire trust and asset management activities at one time. Upon the conclusion of their audit, the auditors will present the results of their audit (usually in one report) to the subsidiaries' audit committee(s).

  OTS does not object to this auditing method as long as the sample includes the functions performed by the savings association entity. However, the trust department audit committee should receive a presentation of findings in accordance with the requirements set forth in §550.480 and ensure monitoring practices are established to correct noted deficiencies.

CHAPTER: Operations, Internal Controls, Audit and Information Technology

SECTION: Audit Examination Program — Section 410P

Examination Objective

To determine the level and quality of the audit process. Consider whether:

- qualified personnel perform the audit function;
- the scope of the audit is consistent with the savings association's size, complexity of operations, level of growth and previous examination findings;
- the fiduciary audit committee or other appropriate committee directs the conduct of the audit;
- the results of the audit are reported to the board and management;
- appropriate actions are taken by management as a result of the audit;
- the audit program strengthens internal controls; and
- internal controls are effective in monitoring management and staff's adherence to policies, procedures and applicable law.

Examination Procedures

Level I Level I procedures first focus on a review of the examination scoping materials. The next step consists of interviews with trust department personnel to confirm their qualifications and levels of expertise; to determine if the trust department's practices conform to written guidelines; to establish whether any significant changes in personnel, operations or business practices have occurred; or whether new products and/or services have been introduced. If items of concern are uncovered during Level I procedures or if problems are identified during the preexamination monitoring and scoping; the examiner may need to perform certain Level II procedures.

1. Review examination scoping materials related to the audit program. Scoping material should include:

    - Risk profile
    - Relevant PERK documents
    - Previous trust and asset management examination report
    - Previous safety and soundness examination report
    - Workpapers from the previous examination
    - Board of director and audit committee minutes
    - Examination reports of subordinate, functionally regulated entities

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

[Click&type]

2. Assess whether an audit committee has been formed and made responsible for directing the conduct of the saving association's trust and asset management activities.

[Click&type]

3. Determine if the audit committee members include officers of the savings association or an affiliate or are members of other committees involved with fiduciary activities.

[Click&type]

4. Review the board of director and the audit committee minutes. Evaluate the level of control of the trust department audit as well as the audit approval process.

[Click&type]

5. Determine if the trust department has been audited according to the approved type of audit program, continuous or annual.

[Click&type]

6. Evaluate whether the auditors have sufficient education and experience to audit trust and asset management activities. Assess whether the savings association has recently changed auditing personnel or firms and discuss with management the reasons for the change. Evaluate evidence of any disagreements between the auditor and the savings association regarding matters of fiduciary principles or practices, internal controls or auditing procedures.

[Click&type]

7. Review the operation of the audit department to determine its functional responsibilities and independence. Determine whether:

   - the auditor approaches the audit process in an ethical and professional manner.
   - management imposes any restrictions on the audit program or places any budgetary or scheduling restraints on the auditors.

[Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

8. If the audit function is outsourced to a third party, determine that the board or audit committee has reviewed the qualifications of the auditor or approved an audit plan or program. Review the engagement letter to determine if the procedures to be performed are clearly stated**.**

[Click&type]

9. Review the audit program and schedule and determine its completeness and compliance with §550.440 - 550.480. Consider:

- Whether the internal audit program is modified in a timely manner to keep pace with changes in trust and asset management activities, economic environment, technology and applicable law.
- Whether the audit program is designated a continuous or annual audit.
- Whether the internal auditor has experience in auditing all types of trust and asset management activities.
- Whether the auditor has established the scope based on an assessment of risk. Evaluate the reasonableness of the assessment. Check for evidence that the auditor has investigated areas with the greatest risk of loss and has allocated sufficient coverage time.

[Click&type]

10. Review audit reports and recommendations by the auditors. Determine whether management, the board and/or the audit committee has approved the recommended changes or provided other satisfactory responses. Also, determine that all noted deficiencies and concerns have been addressed.

[Click&type]

11. Consider whether the following risk contributors (if applicable) have been addressed:

- Significant risks are consistently and effectively identified, measured, monitored and controlled
- The expertise and independence of the audit team is considered adequate
- The quality of the written audit programs, policies and procedures is sufficient
- Corrective action is immediately implemented and monitored

[Click&type]

The completion of the Level I procedures may provide sufficient information to make a determination that no further examination procedures are necessary. If no determination can be made, proceed to Level II.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Level II Level II procedures focus on an analysis of trust department documents such as reports and outsourcing contracts. The examiner should complete the appropriate Level II procedures when the completion of Level I procedures does not reveal adequate information on which to base a conclusion that the trust department meets the examination objectives. Neither the Level I nor the Level II procedures include any significant verification procedures.

1. Determine whether the auditors are free from the influence of management, including performance evaluation and control of salaries.

   [Click&type]

2. Review the distribution of internal audit reports.

   [Click&type]

3. Determine if the auditors have reviewed the savings association's policies and procedures to determine if they adequately cover all areas of trust and asset management activities and comply with applicable law.

   [Click&type]

4. Review and evaluate the educational background and training of auditors.

   [Click&type]

5. Determine if the external auditors have any relationships with the savings association, its directors, officers, employees or other material involvements that would compromise their independence.

   [Click&type]

6. Determine if the external auditors have any stock holdings or borrowings with the savings association.

   [Click&type]

7. Review the external auditor's engagement letter and note any restrictions and/or critical comments.

   [Click&type]

If the examiner cannot rely on the trust and asset management Level I or Level II procedures, or data contained in department records or internal or external audit reports to form a conclusion; proceed to Level III.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Level III Level III procedures include verification procedures that auditors usually perform. Although certain situations may require that Level III procedures be completed, it is not the standard practice of Office of Thrift Supervision (OTS) examination staff to duplicate or substitute for the testing performed by auditors.

1. Evaluate the scope of the auditor's work and review the written audit reports and working papers for adequacy. Determine if the audit reports are adequate, prepared in accordance with the audit program, comply with prescribed procedures and are properly documented. Ensure that the auditor has tested and verified the reliability of information produced in the report.

   [Click&type]

2. Discuss with management the level of problems and identified risk exposure. Focus on the cause of the problems and subsequent risk that has been created.

   [Click&type]

3. Encourage management to enhance their audit program or remove the current auditors.

   [Click&type]

4. Discuss with management the ability of the savings association to commit to specific actions regarding deficiencies.

   [Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Final Risk Assessment

Determine a final risk assessment regarding the audit program of the trust department based on the level of examination conducted.

Type of Risk	Quantity of Risk: High, Medium, Low	Quality of Controls: Effective, Acceptable or Weak	Direction of Risk: Increasing, Decreasing or Stable
Reputation Risk			
Strategic Risk			
Transaction/Operational Risk			
Compliance/Legal Risk			
Financial Risk			

Support the ratings from the matrix above with a concise summary explanation for each of the risk categories as to quantity, quality and direction of risk.

Overall Risk Assessment
[Click&type]

Examiner's UITRS Rating, Summary, Conclusions and Recommendations:

[Click&type]

References - 410P

Laws

Code of Federal Regulations

12 CFR 550	Trust Powers of Federal Associations (General)
12 CFR 550.440	Audit of Fiduciary Activities
12 CFR 550.450	Standards that Govern Audit
12 CFR 550.460	Who May Conduct the Audit
12 CFR 550.470	Fiduciary Audit Committee and Restrictions
12 CFR 550.480	Reporting Audit Results
12 CFR 563c.3	Qualifications of Public Accountant

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Office of Thrift Supervision Publications

Thrift Activities Handbook Sections 350, 355

Other

Workpaper Attachments - 410P

[Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Optional Topic Questions

The following list of questions is offered merely as a tool and reference for the examiner and is not a required part of the examination process.

Audit Committee

• Does the entire board of directors or a distinct audit committee have responsibility for directing the conduct of the savings association's trust and asset management activities?

• If there is a distinct audit committee,
  • Is the composition of the committee in compliance with 12 CFR §550.470?
  • Do any active officers of the savings association or an affiliate serve as a member of the committee?
  • Are a majority of the committee members not members of another board committee delegated power to manage the organization's fiduciary activities?

• Does the auditor report directly to the board or the audit committee?
• Has the audit committee reported in writing to the board the results of the audit, including significant actions taken as a result of the audit?
• Has the audit committee reviewed comments about trust and asset management activities in the most recent OTS report of examination and taken appropriate corrective actions?
• Does the board of directors or audit committee require timely and sufficiently detailed audit reports? Do the audit reports address the auditor's scope for each audit, procedure performed, areas not covered, the justification for the auditor's sample sizes and the basis for each conclusion?

Audit Program

• Has the audit been conducted, either directly or through others, of the savings association's significant trust and asset management activities at least once each calendar year (if annual audit) or at an interval commensurate with the activity's nature and risk (if continuous audit)?
• Has the board devised a satisfactory written audit program?
• Does the board of directors or the audit committee approve the frequency schedule and scope?
• Is the audit function involved in the design or review of major changes in operational procedures?
• Is the audit scope based on a risk assessment of trust and asset management activities?

Program Section - Accounting and Physical Security Controls

• Does the audit program verify account assets annually, including a confirmation from outside custodians?
• Does the program determine whether assets are safeguarded adequately (including unissued stocks, bonds and trust department checks) through the use of dual control? Are trust department assets kept separate from the savings association's assets?
• Does the audit program verify that a written record of vault asset movements is maintained under joint custody?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

• Does the audit program determine whether securities pledged under 12 CFR §550.310 & 320 and 12 CFR §550.490 – 550.510 are adequate, properly safeguarded, held separate and earmarked appropriately on book entry systems?
• Does the audit program use appropriate sampling techniques and verify prompt ledger control of assets?
• Does the audit program verify that cash in trust department accounts is reconciled regularly with demand deposit statement(s)?
• Does the audit program verify that internal balancing control procedures are performed appropriately each time ledgers are posted?
• Does the audit program verify that all suspense or operating accounts are reconciled at least monthly, contain only appropriate items and are cleared in a timely manner?

• Does the audit program verify the proper reconcilement of each of the following to the trust department's general ledger controls at least quarterly:
  • Income cash
  • Principal cash
  • Invested income
  • Invested principal
  • Each type of investment, such as stocks, bonds, real estate loans and real estate
  • Investments by issuer

• Is the bookkeeping system adequate for the volume and nature of business transacted?
• Does the audit program require reconciling or verifying the reconcilement by others of bonds printed to the printer's certificate for each bond trusteeship at least once in each calendar year?
• Does the audit program use appropriate sampling techniques to verify the accurate payment of dividends from dividend disbursing agency accounts by reconciling or verifying the savings association's reconciliation?
• Does the audit program use appropriate sampling techniques to verify the savings association's reconcilement of bond closing statements of new corporate bond trusteeships to trustee records? Reconcilements should include trustee records of bonds authenticated and issued, proceeds from bond sales and initial funding of related accounts.
• Does the audit program use appropriate sampling techniques to verify the accuracy of payments from paying agency accounts by reconciling or verifying the savings association's reconciliation?

Program Section – Activity Control

• Do the auditors verify commissions and fees paid to the savings association and check that they are collected systematically and on a timely basis? Do they ensure that they are properly authorized and correctly calculated?
• Do the auditors compare proceeds from the sale(s) of assets to brokers' invoices, purchasers' receipts or other evidence of sales price?
• Do the auditors compare payment for purchases of assets to brokers' invoices, seller's receipts or other evidence of purchase price?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

• Are disbursements verified to ensure that income and principal distributions are reviewed for accuracy, conformity with the governing instrument and received by beneficiaries or other persons in the proper amount and within the specified time period?
• Do the auditors compare the income receipts from investments with the amounts received for accuracy?
• Do the auditors verify payments for services, such as brokerage fees, real estate management, maintenance charges and similar disbursements with the appropriate bills or invoices?
• Do the auditors verify that combined securities transactions result in equitable distributions in the price and commission among accounts?
• Do the auditors verify that an independent party with the trader's memo and broker's confirmation reconciles securities transactions by price and commission for each security transaction?
• Do the auditors verify that securities transactions are completed within acceptable time limits?
• Do the auditors verify that there is no evidence of excessive trading in managed accounts?
• Do the auditors verify that investment objectives are appropriate for accounts?
• Do the auditors verify that account documentation is appropriately maintained?
• Do the auditors verify that account statements are generated and submitted to an individual independent of the trust department at least annually?

Program Section - Compliance

• Do the auditors verify that transactions with affiliates are in compliance with written agreements and applicable law? See 12 CFR §563.42(b).
• Have the auditors reviewed fiduciary account holdings for compliance with 12 CFR §550.330?
• Do the auditors review the investment of discretionary fiduciary accounts in the stock or obligations of directors, officers and employees of the savings association, its holding company or its affiliates without authorization under applicable law?
• Do the auditors review for compliance with 12 CFR §550.350 regarding loans of discretionary fiduciary account assets to directors, officers and employees of the savings association or its affiliates?
• Do the auditors verify that discretionary accounts are reviewed in accordance with 12 CFR §550.220?
• Do the auditors verify that cash receipts for discretionary fiduciary accounts are invested or distributed promptly in compliance with 12 CFR §550.290?
• Have the auditors checked for compliance with 12 CFR §563.177 and 12 CFR §563.180 (Bank Secrecy Act and suspicious activity reports)?
• Have the auditors verified that products and services purchased with securities brokerage commissions are within the "safe harbor" provision of Section 28(e) of the Securities Exchange Act of 1934?
• Have the auditors reviewed overdrafts to determine the amounts, cause, duration, anticipated date of elimination and adequacy of security, including testing of more than one date? (Note: Overdrafts in ERISA accounts exceeding 3 business days may be a prohibited transaction).
• Have the auditors evaluated the allocation of income and principal for compliance with the governing instrument and state law?
• Have the auditors tested documents necessary for closing accounts, such as discharges, releases, receipts and accountings?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

• Have the auditors tested for compliance with state escheat laws?
• Have the auditors reviewed employee benefit accounts for compliance with Employee Retirement Income Security Act of 1974 (ERISA)?
• Have the auditors determined whether real estate is properly insured, subject to periodic appraisals and inspections, and when appropriate, produces income? Have the auditors tested to ensure that account files are adequately documented?
• Have the auditors determined that supporting papers for real estate loans and contracts are appropriate and accurate?

Program Section - Administrative Audits

• Have the auditors determined whether the original or an authenticated copy of the governing instrument is on file?
• Have the auditors determined if account synoptic and history records are reliable and comprehensive?
• Have the auditors determined whether accounts are administered and invested in conformance with management policies, fiduciary principles, governing instruments and applicable law?
• Have the auditors verified distributions of income and principal for accuracy and conformity with terms of the governing instrument? Distribution receipts should be in the file.
• Have the auditors determined whether written approvals or directions of appropriate parties are obtained promptly?
• Have the auditors determined if tax returns are prepared and filed on time with proper remittances?
• Have the auditors tested the accuracy of account statements submitted to beneficiaries and others?
• Have the auditors determined if board of director minutes, or designated persons and committees, document the review of important matters, such as the acceptance and closing of accounts, investment reviews and discretionary payments of principal or income?
• Do the auditors determine if the board or a board-appointed designee reviews, updates and approves policies and procedures on a regular basis?
• Have the auditors reviewed policies and procedures to determine if they adequately cover all areas of fiduciary activities in which the bank engages and whether they comply with applicable law?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

CHAPTER: Operations, Internal Controls, Audit and Information Technology

SECTION: Introduction to Information Technology Section 500

Introduction to Information Technology

(This section substantially repeats the information provided in Section 341 of the OTS Thrift Activities Handbook.)

Savings associations are becoming increasingly dependent on the use of information technology (IT). Such dependence presents risks to the financial condition and operating performance of the institution that management and the board of directors must effectively manage. Accordingly, in a risk-focused supervision framework, examiners must consider the risks associated with information technology in evaluating the institution's trust and asset management activities and the effectiveness of the risk management process. Significant negative findings should be referred to the OTS regional office and the manager of the IT examination function.

Increasingly, savings associations are focusing on opportunities presented by electronic services, the Internet and the World Wide Web in an effort to remain competitive, improve customer service and reduce operating costs. Consequently, the electronic environment and technology employed by savings associations in connection with the products and services it offers is continually and rapidly evolving. Whether the institution's deployment of technology is limited to the use of personal computers (PCs) or has been expanded to include transactional capabilities over the Internet or account aggregation services for customers, the rapid pace of change in technology calls for increased examiner attention to the IT function.

Regardless of the level of sophistication, risks are inherent in all electronic capabilities. Threats can come from both internal and external sources. Outside hackers, disgruntled employees and inadvertent errors can adversely affect IT reliability. For instance, unauthorized parties may alter an information-only World Wide Web site used for advertising purposes. Electronic mail containing confidential or proprietary information may be accessed or distributed in error. Unauthorized parties might access networked systems that are directly connected to a savings association's main operations database. If these risks are not recognized and the subsequent problems promptly detected and addressed, they can lead to significant monetary and reputational losses for a savings association.

Operating Environment

Savings associations have a number of choices available to meet their constantly changing and evolving information system and technology needs. Most savings associations use one or more of the following sources to deploy and operate systems and technology:

- Personal computers and local and wide area networks
- An in-house computer center and client server system
- Outsourced vendors

A savings association's decision to select the appropriate information technology strategy can depend on several factors:

- In-house expertise;
- Capital to acquire the necessary resources;
- Facilities to house the resources;
- Cost of outsourcing to vendors; and
- Management's ability and willingness to use information technology to build a competitive advantage within a safe, sound and secure infrastructure.

Personal Computers and Local and Wide Area Networks

The personal computer has become a prominent tool in today's business environment. It is used in information processing in either a stand-alone or network arrangement. Local and wide area networks of PCs have offered substantial benefits in productivity and information access. Institutions growing use of PCs to deploy new technology is dependent on a network environment. The electronic network facilitates interaction between the savings association and the users (staff and customers). Telephone banking, PC banking, automated teller machines, automatic bill payments, and automated clearinghouse systems for direct deposit or payment, are familiar examples of existing and evolving services that savings associations can offer to their customers through an electronic network. Such access, however, also means that those control procedures, previously limited to the central operations, must be reapplied and extended to the PC user level.

Basic controls and supervision of PCs often have not been introduced or expected at the PC user level. The technological advantages, expediency and cost benefits of the PC have been the primary focus. Recognition of the increased exposure has not kept up with the demand for expanded information processing power.

While each PC requires certain operational type controls such as physical security (lock and key), logical security (password) and file backup, the more pronounced risks involve those operations using PCs as stand-alone processors.

PC users frequently engage in program development directly on their desktop computers. This may involve the original creation of a software program or the customization of existing routines from vendor software. With both methods, adequate control techniques for the programming, testing and documentation are necessary to ensure the integrity of the software and the production of accurate data.

PC users can also perform other functions separate from any centralized operating controls. For example, users can download and manipulate information from main databases. They can also originate data. Each of these activities can create information that management will use in making decisions that affect corporate strategies and customer relationships. Therefore, the evolution of the PC-based system has not eliminated the need for adequate operating controls. Rather, the focus of control was shifted to the PC user level.

In-house Computer Centers and Client Server Systems

In-house computer centers vary in size and complexity, type and number of data processing professionals, number and types of applications processed, transaction volume, and processing deadlines. Computer equipment may vary in size from large "mainframe" to smaller microcomputer systems. For example, in-house information systems used to generate revenues, such as loan origination systems, are frequently operated on microcomputer-based systems. Software for in-house computer systems may be purchased or licensed from outside vendors or developed internally.

Less expensive and faster computers have resulted in the emergence of client server technology. While stand-alone mainframe or personal computers make it difficult to share information with other information systems, client server technology allows a savings association to link multiple computers together to provide enough power to allocate data processing capabilities to a network. High-speed data transmission and network file servers are common characteristics in a client server computing environment.

Outsourcing

Some savings associations may determine that their need of information technology is too sophisticated or dynamic for effective support by internal resources. These institutions may determine that some or all of their technology needs should be outsourced to a facilities management company, service bureau or other third-party contractor.

This delegation does not lessen the burden on management to supervise and control all aspects of the savings associations' IT activities. An institution's delegation of responsibilities through outsourcing requires reasonable due diligence efforts throughout the term of the engagement. Conditions, rights and responsibilities of the savings association and the vendor should be governed by written agreements. This is particularly important in an electronic environment because short-term engagements, new developments and untested entities are not uncommon. Further, management must coordinate all outsourcing arrangements to ensure that security, reliability and integrity are not compromised. Examiners should ensure that all outsourcing arrangements are executed with the same access, control, monitoring and reporting environment that would be expected for a savings association with proprietary systems.

Service Bureau

Service bureaus provide standardized information system services to multiple institutions. They are common among smaller savings associations with a limited number of customer accounts and low transaction volume. Due to the costs and technical resources required to maintain an in-house computer center, some larger savings associations also find service bureaus a cost-effective alternative. Service bureaus provide the savings association with experience, proven software and reliable hardware.

Typically, data is forwarded to the service bureau computer center via on-line data entry terminals or by tape, diskette or paper copy transported by courier. Output reports are returned to the savings association in the same manner. A regulator appointed by the FFIEC examines major service bureaus providing service to federally regulated financial institutions. Savings associations should ensure they receive copies of the service bureau's IT examination report.

Contracts

When employing the services of an outside vendor, management should carefully review any proposed service contracts or agreements with an eye toward minimizing the savings association's exposure to risk. The guidelines listed below should be considered when executing any contract with an outside vendor. In addition, the savings association's legal counsel should review the draft contract to determine that the interests of the institution are adequately protected. Some guidelines when contracting with an outside vendor are to:

- Consider the following points prior to entering into any service arrangement:
  - Alternative vendors and related costs
  - Financial stability of the vendor
  - Requirements for termination of service
  - Quality of the service provided
- Ensure that any contract specifies the duties and responsibilities of the savings association and the service provider.
- Review the contract's penalty provisions for reasonableness in the areas of contract length, fees and compensation of the savings association for loss of income.
- Ensure that the following items are included in the service contracts:
  - The service provider agrees to submit to an examination by OTS, which will evaluate and monitor the soundness of the provider in order to limit the savings association's risk. Specifically, the following language should be incorporated in the contract:

    > "By entering into this agreement, the service provider agrees that the Office of Thrift Supervision will have the authority and responsibility provided to the other regulatory agencies pursuant to the Bank Service Corporation Act, 12 U.S.C. 1867(C) relating to services performed by contract or otherwise."

  - The service provider provides the OTS regional director of the region in which the data processing center is located, a copy of any current third-party review and the current audited financial statements.
  - The service provider agrees to release the information necessary to allow the savings association to develop a contingency plan that will work in concert with the service provider's plan.

Management Controls for Evaluating and Controlling Risks

Savings associations should adopt a risk management program to address unique aspects of an electronic environment. While most deficiencies in information technology tend to be directly related to operational risk, information technology also can affect other business risks (credit, market, financial, legal and reputation) depending upon the specific circumstances. Information technology elements should be viewed in an integrated manner with the overall business risks of the institution and its business lines and products. A deficiency in any one of the IT elements could have a substantive adverse effect on the institution.

The risk-focused supervisory process places emphasis on the evaluation of information technology and its effect on an institution's trust and asset management operations. Accordingly, examiners should specifically consider information technology when developing risk assessment and supervisory plans. They should determine the appropriate level of review of IT activities given the characteristics, size and business activities of the institution. In general, examiners should:

- Develop a broad understanding of the institution's approach, strategy and structure with regard to information technology. This requires a determination of the role and importance of information technology to the institution and any unique characteristics or issues.

- Incorporate an analysis of information technology systems into risk assessments and action plans. The analysis should include identification of critical information technology systems, related management responsibility and the major technology components. An organization's information technology systems should be considered in relation to the size, activities and complexity of the organization, as well as the degree of reliance on these systems.
- Assess the institution's critical systems, that is, those that support trust and asset management activities and the degree of reliance those activities have on information technology systems. The level of review should be sufficient to determine that the systems are delivering the services necessary for the institution to conduct its business in a safe and sound manner.
- Determine whether the board of directors and senior management are adequately identifying and controlling the significant risks associated with information technology for its trust and asset management business line.

An effective risk management control program will minimize the negative effects of a problem situation. Minimizing the potentially negative effects can be particularly difficult in an electronic environment that offers speed, sophistication and access to many users, regardless of their legitimacy. Further, because systems will likely affect all activities to one degree or another, a single problem can have an effect on several areas including product management, marketing, customer service and operations.

For instance, electronic advertising can provide information about products, services, rates and fees. Incorrect information can lead to customer complaints, contingent liabilities or lost opportunities and income. As a result of unauthorized system access, content may be altered to include inappropriate material that can be viewed by the general public. If the savings association has weak controls and security, users may be able to access, disclose or improperly use confidential information.

Practices to Control Risks

- Input and Output Controls

  Control practices that govern input and use of information are important to safeguard. Historically, control weaknesses have contributed to fraud and recordkeeping problems. Most operational charge-offs can be traced to problems related to the input and use of information.

  A savings association should require specific data controls for technology that is used to process information that has a direct monetary effect on the institution or its trust and asset management customers. At a minimum, these controls should include the requirement that there be a segregation of duties between the input of information and the review of that information after it is processed. Such controls should also require the reviewer to reconcile the processed information. Institutions should require that most functions relating to processing assets be performed under dual control. Appropriate controls should be established in the early stages of development and deployment and described in detail in the savings association's operating policies and procedures.

  The savings association should also establish data editing routines to help ensure that data entering a system is error-free. This control is important whether the data is being manually entered or electronically transferred from another system.

- Information Security

  The savings association should have a security system in place that controls access by unauthorized internal or external users. With the increasing use of personal computers and local and wide area networks, it is possible for an institution to expand access to applications and data to all staff. As the number of users increases, however, so does the threat of unauthorized use. Similarly, activities conducted through other interactive devices, such as the Internet, automated teller machines, telephones and televisions, open the computer system to outside and potentially unauthorized users. Although the access devices and distribution channels vary, the issues are the same regardless of the type of access device or distribution channel.

Management should control access to prevent a security compromise of its systems. Data is particularly vulnerable to unauthorized access or alteration during transmission over public networks. Management should develop methods to maintain confidentiality, ensure that the intended person receives accurate information and prevent eavesdropping by others. In addition, evidence of participation by both the sender and the receiver in a transaction should be created.

Effective security does not rely on one solution, but on several measures that, together, serve to identify and control risk. Although not all-inclusive, the following potential risks and mitigating controls should be considered in developing a system security program:

Authorization: Authorization involves the predetermination of permissible activities. Management should ensure that customers have access only to their own accounts and perform only authorized functions.

Access Controls: Traditional access controls, such as user identification, passwords and personal identification numbers, should be implemented for all users. However, since the effectiveness of these controls is greatly influenced by the user, management should take all possible steps to educate the user in this area. For example, new users typically use their name or social security number as a password or write their password on a piece of paper for ease of reference. Management should educate users on the risks of such practices and promote the use of alphanumeric passwords.

Secure Data Storage: Confidential information or highly sensitive data should be stored securely. Management should consider storing sensitive data in encrypted form and implementing stringent access controls.

Encryption: Encryption technology disguises information to hide its meaning and enhances confidentiality by restricting information access to intended users. Encryption-based methods can also be used to verify message authenticity and accuracy. Information is encrypted and decrypted with a cipher and key using specialized computer hardware or software. Secrecy of the key and complexity of the cipher are crucial for the success of encryption controls.

Firewalls: Firewalls are physical devices, software programs, or both, that enhance security by monitoring and limiting access to computer facilities. They create a security barrier between two or more networks to protect the computer system from unauthorized entry.

Authentication: Authentication controls are used to verify and recognize the identity of parties to a transaction. Such controls typically include acknowledgment, computerized logs, digital signatures, edit checks and separation of duties. Weak authentication controls can allow the accuracy and reliability of data to be compromised by unauthorized fabrication, errors introduced in the system or corruption. Savings associations should utilize authentication controls to preserve the integrity of data.

Acknowledgment: Acknowledgment controls include batch totaling, sequential numbering and one-for-one checking against a control file to verify that electronic transactions are properly completed. For example, if an electronic transmission is interrupted, the institution should have controls to notify the sender of the incomplete transaction and prevent duplication of data during the retransmission. In addition, savings associations should install anti-virus software to prevent corruption of data or systems.

Evaluating Information Technology

The trust and asset management examiner should focus on the systems and issues that are considered critical to the performance of the institution's trust and asset management responsibilities. There are five basic IT elements to be considered in the discussion of the risks associated with information technology. While trust and asset management examiners will defer to the OTS information technology examination staff for a more technical review of these elements, the trust and asset management examiner should discuss them with management to ascertain whether the appropriate risk controls have been established. The five information technology elements are:

Management Processes: Management processes encompass planning, investment, development, execution and staffing of information technology from a corporate-wide and business-specific perspective. Management processes relating to information technology are effective when they are aligned with, and supportive of, the institution's mission and business objectives. Management processes include strategic planning, management and reporting hierarchy and a regular independent review function.

Architecture: Architecture refers to the underlying design of an automated information system and its individual components. The underlying design encompasses both physical and logical architecture, including operating environments and the organization of data. The individual components refer to network communications, hardware, operating systems software, communications software, database management systems, programming languages and desktop software. Effective architecture meets current and long-term organizational objectives and addresses capacity requirements to ensure that systems allow users to easily enter data at both normal and peak processing times. It also provides satisfactory solutions to problems that arise when information is stored and processed in two or more systems that cannot be connected electronically.

Integrity: Integrity refers to the reliability, accuracy and completeness of information delivered to the end-user. An information technology system has an effective level of integrity when the resulting information flows are accurate and complete. Lack of integrity in an institution's systems will adversely affect day-to-day reliability, processing performance, input and output accuracy and ease of use of critical information.

Security: Security refers to the safety afforded to information and its data processing environments, using both physical and logical controls to achieve a level of protection commensurate with the value of the information. Information technology has effective security when controls prevent unauthorized access, modification, destruction or disclosure of information during its creation, transmission, processing, maintenance or storage.

Availability: Availability refers to the delivery of information to end-users. Information technology is effective only when information is consistently delivered on a timely basis to support business and decision-making processes. In assessing the adequacy of availability, examiners should consider the capability of information technology to provide information to the end-users from either primary or secondary sources, including contingency plans to mitigate business disruption. Contingency plans should set out a process for restoring or replacing its information processing resources, reconstructing its information assets and

resuming its business activity when disruption occurs. Disruption may be caused by human error or intervention, natural disaster or infrastructure failure (such as loss of utilities or communication lines) or operational failure of hardware, software or network communications.

Contingency Planning

All institutions should have written contingency plans established in the event that data is lost or systems are damaged. The contingency plans should address processes to restore data and systems from off-site backup. Contingency planning, also known as business resumption planning, is a process of reviewing an institution's departments or functions and assessing each area's importance to the viability of the organization. This planning process should address each critical system and operation, whether performed on-site or by a service provider.

The savings association's board of directors and senior management are responsible for the comprehensive planning, review, testing and approval of the institution's contingency plans. These plans should be reviewed annually and documented in board minutes.

If the savings association has contracted with a service provider, management also must evaluate the adequacy of contingency plans for its service provider and ensure that the savings association's contingency plan is compatible with its service provider's plan.

Contingency plans can minimize business disruptions caused by problems that impair or destroy the institution's processing and delivery systems. The loss or extended disruption of business operations poses substantial risk of financial loss and could lead to the failure of the institution. Therefore, contingency planning requires a department-specific, as well as an institution-wide emphasis, as opposed to focusing only on the centralized computer operations.

The beginning point in establishing a contingency plan is to assess the risks posed by each processing system, identifying the principal departments, resources, activities and constituencies potentially affected. This includes assessing the response capability of service vendors that provide disaster recovery services. The vendor should provide alternative processing sites as well as storage and transportation of back-up media between the storage vendor, alternate processing site and the institution). Management should also formally appoint and empower individual(s) with the latitude and authority to respond during an incident.

The savings association's contingency plan should also include an incident response team. Generally, the team consists of the officers and employees who represent key departments and functions and who collectively provide the expertise necessary to respond quickly and decisively to problems. A preparedness plan should also be established that defines the roles and responsibilities for each team member. Although the degree of sophistication will vary depending on the risks inherent in each system, establishing an incident response team and preparedness plan also provides a platform from which an institution can respond to a problem situation. The composition of a response team or extent of a preparedness plan will depend upon the level and complexity of information technology and the institution's available resources.

Distinction Between Information Technology and Trust and Asset Management Examiner Review

Information technology examiners will continue to examine savings associations that operate their own computer center or have sensitive and complex internal information systems operated on personal computers or local or wide area networks. Additionally, IT examiners will continue to examine national, regional and local service bureaus. All information systems examinations (institution and service bureau) are conducted

according to the policies and procedures in the Federal Financial Institutions Examination Council (FFIEC) Information Systems Examination Handbook.

Trust and asset management examiners will examine the information systems and technology controls of savings associations that have information system services provided primarily by a service bureau but are increasingly using internal information systems and technology to perform daily operations and provide products and services. During the course of a trust and asset management examination, examiners should specifically review the adequacy of authority level controls and access to Fedline operations in the trust department.

In addition to these procedures and those found in Section 341 of the Thrift Activities Handbook, examiners should become familiar with the FFIEC Information Systems Handbook as a source of useful information.

Examiners are reminded that access and speed capabilities can magnify risk in an electronic environment. This is particularly true if risk management control programs are ineffective or if a system is linked to a savings association's central operations or databases. In other words, a savings association can be exposed to significant risk even if activity volume is nominal. Therefore, consultation between the trust and asset management and IT examiners may be necessary to comprehensively evaluate a savings association's electronic environment. Trust and asset management examiners should consult with a regional IT examiner for assistance, as necessary.

Generally, the need for services of an IT examiner may include instances where:

- The savings association has a web site that is directly connected to its operating system
- The savings association has the capability for customers to access and transfer data, files or messages
- The savings association has the capability to enable users to direct or process financial transactions (e.g., transactional web site or stored value system)
- Significant deficiencies or weaknesses are noted
- Systems are unusually sophisticated

Depending on the extent of internal control weaknesses, the examiner in charge (EIC), the trust and asset management examination manager, and the IT examinations manager will determine if follow-up by the IT examination staff is required as part of the current or future examinations.

CHAPTER: Operations, Internal Controls, Audit and Information Technology

SECTION: Information Technology Examination Program — Section 510P

Examination Objective

To determine the adequacy and/or effectiveness of the trust department's information technology. Consider whether:

- the risks involving the savings association's use of electronic capabilities have been analyzed;
- compliance with applicable law is considered;
- credible management reports are prepared and good oversight practices are apparent;
- quality policies, procedures and internal controls are established to monitor and control information technology risk;
- good physical security controls are maintained; and
- deficiencies are identified and prompt corrective action initiated.

Examination Procedures

Level I Level I procedures first focus on a review of the examination scoping materials. The next step consists of interviews with trust department personnel to confirm their qualifications and levels of expertise; to determine if the trust department's practices conform to written guidelines; to establish whether any significant changes in personnel, operations or business practices have occurred; or whether new products and/or services have been introduced. If items of concern are uncovered during Level I procedures or if problems are identified during the preexamination monitoring and scoping; the examiner may need to perform certain Level II procedures.

1. Review examination scoping materials related to information technology functions of the trust department. Scoping material should include:

    - Risk profile
    - Relevant PERK documents
    - ECEF reports
    - Previous trust and asset management examination report
    - Workpapers from the previous examination
    - Previous safety and soundness examination report

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

- Previous safety and soundness IT Program 341
- Information technology examination report, if conducted

[Click&type]

2. Evaluate the information technology policies and procedures for adequacy. Consider whether they address:

   - Information integrity
   - Operations technology
   - Vendor management
   - Internet services
   - Electronic mail
   - Critical file backup
   - Contingency planning

   From the evaluation, assess the information technology infrastructure including local area networks (LANS), wide area networks (WANS) and other information technology resources.

   [Click&type]

3. Determine if significant changes to outsourcing arrangements have occurred.

   [Click&type]

4. Evaluate whether management has the knowledge and expertise to manage its information technology. Determine if any significant personnel and/or organizational changes occurred.

   [Click&type]

5. Determine the role and importance information technology plays within the organization and whether this presents any unique issues. Assess whether the savings association's use of information technology is appropriate to the size and complexity of the trust department.

   [Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

6. How does management monitor the performance of all third party service providers? Assess management's due diligence and vendor selection process.

[Click&type]

7. Determine whether any new information technology type products or services have been installed. Also, determine whether any new trust and asset management services required new or an adaptation of existing technologies. Consider whether:

- internal audit assessed the new systems or programs prior to implementation;
- management maintained the level of expertise necessary to manage these technology products and services;
- technological advances are kept up with, such as online payment, digital signatures and/or wireless technology;
- information systems are protected from external intrusion; and
- system reliability and performance are considered.

[Click&type]

8. Has an audit or other review been performed on all service providers? Did management obtain a copy and review the results?

[Click&type]

9. Assess the adequacy of audit coverage of the trust department's information technology. Determine whether information technology audit plans and audit schedules are commensurate with the department's information technology environment and risks.

[Click&type]

10. Consider whether the following risk contributors (if applicable) have been addressed:

- Does management fully understand all aspects of information technology?
- Does management anticipate and respond well to market and technological change?
- Do management information systems and reports provide credible and comprehensive information?
- Are prudent due diligence efforts used in the selection of service providers when this function is delegated?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

- Does management quickly identify weaknesses and take appropriate action?
- Do material, unresolved issues noted in audit, compliance or examination reports remain uncorrected?
- Do policies and procedures address all significant activities?

[Click&type]

The completion of the Level I procedures may provide sufficient information to make a determination that no further examination procedures are necessary. If no determination can be made, proceed to Level II.

Level II Level II procedures focus on an analysis of trust department documents such as reports and outsourcing contracts. The examiner should complete the appropriate Level II procedures when the completion of Level I procedures does not reveal adequate information on which to base a conclusion that the trust department meets the examination objectives. Neither the Level I nor the Level II procedures include any significant verification.

1. Review the savings association's web site as it relates to trust and asset management activities. If the website is a transactional website, confirm that the savings association notified OTS and was granted approval.

   [Click&type]

2. Review the savings association's policies and procedures to determine whether there is adequate security to prevent unauthorized access and entry to customer information and accounts. Evaluate if the web site is managed in a secure manner.

   [Click&type]

3. Determine if management verified the accuracy and content of financial planning software or interactive programs (between internal and external users) available through deployed systems.

   [Click&type]

4. Determine if the savings association's contingency plan addresses information technology as it relates to trust and asset management activities.

   [Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

5. Assess the guidance for employees pertaining to information integrity. Does it address the need to protect the confidentiality of customer and corporate information?

   [Click&type]

6. Is there a segregation of duties among system developers and operations personnel?

   [Click&type]

7. Has management kept up with marketplace changes such as decimalization and has it planned for future changes such as T+1 settlement and straight through processing?

   [Click&type]

8. If the savings association operates a fedline terminal in the trust department, are there procedures in place to ensure that controls are adequate?

   [Click&type]

9. Review all exception reports. Assess management's actions and determine whether the exceptions pose any significant risk to the savings association.

   [Click&type]

10. If there are unresolved exceptions present in internal, external, compliance or examination reports, discuss corrective action with management.

    [Click&type]

If the examiner cannot rely on trust and asset management Level I or Level II procedures or data contained in department records or internal or external audit reports to form a conclusion; proceed to Level III.

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Level III Level III procedures include verification procedures that auditors usually perform. Although certain situations may require that Level III procedures be completed, it is not the standard practice of Office of Thrift Supervision (OTS) examination staff to duplicate or substitute for the testing performed by auditors.

1. Determine if the findings of the audit/compliance review are consistent with examination findings. If not, discuss with management the reasons for any discrepancy.

   [Click&type]

2. Do the operating systems contain sufficient firewalls?

   [Click&type]

3. Are criminal background checks of key IT employees and contractors performed?

   [Click&type]

4. Is there an immediate revocation of system access rights for ex-workers?

   [Click&type]

5. For electronic funds transfers, compare the daily reconcilement of wire transfers with correspondent and general ledger accounts to detect any errors or misapplications of funds.

   [Click&type]

6. Determine if someone with proper authority has been given responsibility for assigning qualified individuals as users of fedline terminals. Determine if passwords are changed frequently and only legitimate users have access to the terminals. Determine if dual controls have been implemented. Determine if terminated employees are promptly removed from accessibility.

   [Click&type]

7. Determine if there is an adequate procedure for backing up critical files. Test the process to determine whether it is being followed. Consider whether diskettes containing significant or critical information are labeled and stored in a secure location (on- or off-site).

   [Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

8. If there are significant examination concerns, contact the OTS information technology examination division.

[Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Final Risk Assessment

Determine a final risk assessment regarding the trust department's information technology environment based on the level of examination conducted.

Type of Risk	Quantity of Risk: High, Medium, Low	Quality of Controls: Effective, Acceptable or Weak	Direction of Risk: Increasing, Decreasing or Stable
Reputation Risk			
Strategic Risk			
Transaction/Operational Risk			
Compliance/Legal Risk			
Financial Risk			

Support the ratings from the matrix above with a concise summary explanation for each of the risk categories as to quantity, quality and direction of risk.

Overall Risk Assessment
[Click&type]

Examiner's UITRS Rating, Summary, Conclusions and Recommendations:

[Click&type]

References - 510P

Laws

Code of Federal Regulations

Office of Thrift Supervision Publications

TB 11-1 Purchased Software Evaluation Guidelines

Other

FFIEC Information Systems Handbook

Workpaper Attachments - 510P

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

[Click&type]

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

Optional Topic Questions

The following list of questions is offered merely as a tool and reference for the examiner and is not a required part of the examination process.

Audit Process

- Does the auditor have specialized information systems audit training?
- Is the scope of the audit program commensurate with the extent of information systems activities? Does the audit program concentrate on issues such as contract administration, insurance, operational controls, on-line access controls, contingency planning and PC/LAN/WAN controls?
- Does the audit program test balancing procedures of automated applications including the disposition of rejected and unposted items?
- Does the audit program sample customer record files (master files) to verify them against source documents for accuracy and authorization?
- Does the audit program spot-check computer calculations such as fee charges, past due loans, etc.?
- Does the audit program verify output report totals, check the accuracy of exception reports, trace transactions to final disposition to determine adequacy of audit trails and perform customer confirmations?
- Do the audit procedures cover the flow of critical data through interrelated systems from the point of origin to point of destination?
- Does the audit process include a review of the servicer's third-party review report? If so, is an evaluation made of any exceptions and recommended corrective action?

Outsourcing Arrangements

- Are outsourcing arrangements with vendors and subcontractors included in the savings association's compliance reviews?
- Determine if management investigates and documents its selection process for new service providers? Does it include the following:
  - Alternative services?
  - Pricing of services, including special charges for forms, equipment, etc.?
  - Quality of reports and user documentation?
  - Financial stability of the servicer?
  - Contingency planning?
  - The ability of the servicer to handle future processing requirements?
  - Requirements for termination of service?
  - Insurance requirements?
  - Review of service contract by savings association's legal counsel?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

- Does the servicer provide the institution with current, understandable user instruction manuals for each application and do the employees use them?

- Determine whether the service contract provisions include:
  - Description of work performed and time schedules for processing and delivery of work.
  - Fee schedules and other charges.
  - On-line communication access and security.
  - Audit responsibility.
  - Opportunities for the savings association to review independent annual audits and similar reports.
  - Provisions for contingency backup processing and record protection.
  - Notice required (both parties) for termination of service and the return of customer records in machine-readable form.
  - Confidentiality of data files and programs.
  - Insurance carried by the servicer.
  - Liability for documents damaged or lost in transit.

- Determine whether the contract administration policies and procedures provide for monitoring and management of the information system service provider's performance in areas such as:
  - Service level performance and service charges
  - Financial condition
  - Ability to meet future needs
  - Performance reports by information system service provider

- Are there reasonable requirements for periodic due diligence reviews of third-party providers, including contractors, subcontractors, support vendors and other parties?

Operations Technology

- Are procedures in place to control customer transfers of funds from each access point?
- Are safeguards in place to detect and prevent duplicate transactions within each system deployed?
- Do policies and procedures address the savings association's use of electronic mail?
- Do policies and procedures address transmissions among all user groups, including customers, officers and employees?
- Are file maintenance changes to customer account record files (master files) requested in writing (Note: In on-line systems, this procedure is handled as part of the system access controls and supervisory override feature)? Are the changes and requests reviewed by staff and, when appropriate, a supervisor? Are the changes verified for correctness after processing?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

- Are microfilm, digitized records, paper copies of checks and data entry source documents secured? If so, verify that:
  - Documents and microfilm/microfiche are stored on- or off-site in a secure location with limited access;
  - An inventory or usage log is maintained at the storage site location and the quality of the microfilm is checked periodically.

Critical File Backup

- Does the savings association have procedures and a training program to promote awareness on the use and care of PCs?
- Is the trust department processing significant applications on a PC and reconciling the input and output for accuracy?
- If yes, has the department developed a security policy that contains minimum control standards for PCs as described in Thrift Bulletin 29 End-User Computing?
- Is there an established program for ongoing review of each system used for content, continued appropriateness, accuracy, integrity, security, controls, system updates, obsolescence, system capacity and strategic direction?

Information Security

- For interactive systems, does management require a review of the interactive components and processes to ensure compatibility and security?
- Has senior management established appropriate levels of access to information and applications for officers, employees, system vendors, customers and other users? Are access levels formally established and reviewed on a regular basis?
- Have appropriate procedures been established to monitor for unauthorized attempts to access the savings association's system? Verify that policies require formal reporting in the event of attempted or actual attacks against any of the savings association's systems.
- Are terminals with service provider access controlled by user logon codes, passwords known only to specified individuals or encryption and when necessary, physical keys and physical configuration?
- Are users with terminal access controlled by unique user log-on codes or passwords known only to the user?
- Is access to PCs restricted due to physical security (keyboard locks, secure rooms) and software security (passwords) and enforced?
- Are PCs linked to a LAN or WAN? If so, are passwords used to grant access and functional authorization on the system? Are passwords changed periodically? Does each user have a unique user identification code and password?
- Have periodic changes been made to user log-on codes, passwords and supervisory override passwords? Are they adequately controlled with regards to personnel authorized to make changes, the security of documentation and monitoring and reporting of violations?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

• Are users or terminals controlled as to the applications they can access, the transactions they can initiate, and specific hours of operation? • Are there sign-off procedures or an automatic sign-off after a period of inactivity?
• Are security passwords and user identification codes suppressed on all video and printed output displays?
• Does the trust department have any direct connection between its internal operating system(s) and the system that hosts the external electronic service or activity (for example, a Web site)? If the savings association does have a direct connection, an IT examiner should be consulted.
• Does the trust department establish the legitimacy of each party requesting an account action or submitting related instructions or data?

• Are appropriate exception reports generated and reviewed on a periodic basis? In addition, do the reports indicate:
  • All transactions made at a terminal by an operator
  • Restricted transactions
  • Correcting and reversing entries
  • Dates and times of transactions
  • Unsuccessful attempts to access the system and restricted information
  • Unusual activity

Web Site

• Has the savings association incorporated a web site in its business plan?
• Has management assessed the annual operating and maintenance costs (including telecommunications, hardware, software, personnel, etc.) in operating a web site?
• Do the savings association's policies and procedures address authentication concerns relating to those customers that may not physically visit the savings association?
• Do the savings association's policies and procedures address fraud and how it will deal with those situations perpetrated outside its geographical area and/or legal jurisdiction?
• Does the trust department have encryption techniques used to process all data, from the end-user personal computer back through the firewall (or DMZ) and to the main data processing site? Refer review of complex web site technology to IT examination staff.
• Are account inquiries and fund transfers processed end-to-end? (If website is "transactional" refer to IT examinations staff.)

Contingency Plan

• For contingency planning purposes, is there a backup system or method established for users to conduct normal activity in the event the system is not available for an extended period of time?
• Are there instruction guides and other support materials that address the backup system or method?
• Has management established a reasonable procedure to notify users in the event of a problem?
• Is the saving association's plan compatible with its service bureau's plans?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____

• Does the plan identify all critical resources, including data communication networks?
• Does the plan provide for in-house communication hubs?
• Does the plan require the savings association to participate in service bureau disaster recovery tests?

Exam Date: _____
Prepared By: _____
Reviewed By: _____
Docket #: _____